Advances in Human Factors of Transportation, Vol. 148, 2024, 697–706
https://doi.org/10.54941/ahfe1005262

Assessment of Resilience in a Maritime Autonomous Transport System

Odd Erik Mørkrid, Kay Fjørtoft, Marianne Hagaseth, and Even Ambros Holte

SINTEF Ocean AS, Trondheim, Norway

ABSTRACT

Resilience attributes are turned upside down when introducing autonomous maritime transport systems, as technology replaces or assists human functions. We enter an unknown world where we need to rely on autonomous functions and the collaboration between humans and technology. Since less human interaction might cause challenges and effects not yet uncovered, Kaber (2018) and Fjørtoft et al. (2023) discussed levels of autonomy in the context of human automation interaction (HAI). The paper particularly looks at the use of levels of autonomy as taxonomies to structure and improve analysis of human performance, workload, but also situational awareness as well as some of the problems that this may cause. The introduction of increasing automation changes the way human and machine interact in many ways. As such, to ensure resilience in autonomous transport systems, these human and machine interaction challenges must be addressed and systemized, and in this paper the different awareness categories humans, technology and external (Fjørtoft, 2021), are revisited and linked to resilience. Also, as an extension on how to utilize integrated planning for autonomous transport systems (IPA), as presented by Fjørtoft et al. (2023), this paper further details emerging issues related to human and machine interface by presenting a framework for how to secure resilience during the design, plan and follow up autonomous ship operations. In other words, the ability to assess and ensure resilience when planning operations in autonomous maritime transport system, while accounting for the interaction between humans and technology. This is of particular relevance due to the likelihood of vessels sailing with different degrees of autonomy, depending on the ongoing operation and its surroundings. Described as operational envelopes in "Towards approval of autonomous ship systems by their operational envelope" (Rødseth, 2021), the overall operation must be broken down into sub-operations such as sailing in open seas, berthing, cargo loading/unloading (crane operation), etc. The framework is exemplified through a case study, by combining research results from the Norwegian project MARMAN and EU projects like AUTOSHIP and AEGIS.

Keywords: Resilience, Human factors, Autonomous maritime transport systems

INTRODUCTION

The digital and autonomous transformation of the maritime industry is well under way. This includes more data available for decision-making, as well as for control on automated and autonomous operations. This paradigm, shift where technology gets a more central role in operations threatens our trust in systems and operations. Hence, the collaboration between humans and technology needs to be assessed in a different way than traditionally. This paper aims to describe how the collaboration between humans and technology can be modelled, how threats of a disrupting event can be understood, but also how barriers should be introduced to mitigate possible consequences. When talking about safety, security and resilience, different terminologies are often used. In this paper we have studied a transport system's proactive and reactive ability to deal with disruptions to reduce the probability of operational incidents and have used the following definitions:

- **Safety**: Reduce the probability of unwanted events and mitigate the consequences of an unwanted event related to safety. Resilience is not safety BUT safety incidents may lead to disruptions.
- **Security:** Reduce the probability of unwanted events and mitigate the consequences of unwanted events related to security. Resilience is not the same as security BUT security incidents may lead to disruptions.
- **Resilience**: Mitigate the consequences of unwanted events and return to normal service as soon as possible. You may not be able to avoid unwanted events but knowledge of the threats leading to the unwanted event may be crucial in the recovery phase.

When designing, planning, and executing operations in a highly automated transport system, where humans interact closely with technology, there is a pressing need for ensuring safety, security, and resilience. This is best ensured by applying holistic planning of the transport system.

A COMBINED FRAMEWORK FOR ASSESSING RESILIENCE IN A MARITIME AUTONOMOUS TRANSPORT SYSTEM

Assessing the resilience in a maritime autonomous transport system is a complex task and new ways of thinking must be established. Several projects, such as the Horizon 2020 project AEGIS[1] and the Norwegian project MARMAN[2] have investigated this matter, (e.g. Fjørtoft et al., 2023), where a new methodology for assessment of resilience in automated transport systems was introduced. However, the methodology lacks the ability to assess in detail the interactions between humans and technology, but also how the identified challenges ought to be addressed and systemized.

Hence, the main objective of the suggested framework is to assess the transport system and to build reliability through identifying threats and vulnerabilities. Another important contribution is that it secures a structured process of how to build operational robustness. The norm is that there are different systems, different stakeholders, different means, and load units involved, with different owners and managers that must be integrated and hence, also able to collaborate. This is crucial when introducing more automated technology or autonomy to the chain, which will generate a completely new way of operating where collaboration between human and technology

[1] https://aegis.autonomous-ship.org/

[2] https://www.sintef.no/en/projects/2021/marman-maritime-resilience-management-of-an-integrated-transport-management/

is essential. The framework consists of three main parts, where the first is an extended version of the bow-tie method for hazard analysis. Its main objective is to identify preventing and reacting barriers of a possible unwanted event, but also visualizing safety-related measures. The bow-tie diagram lists threats on the left side, the top event in the middle, and possible consequences on the right-hand side, Figure 1.

The methodology shown in Figure 1 is depicting six steps:

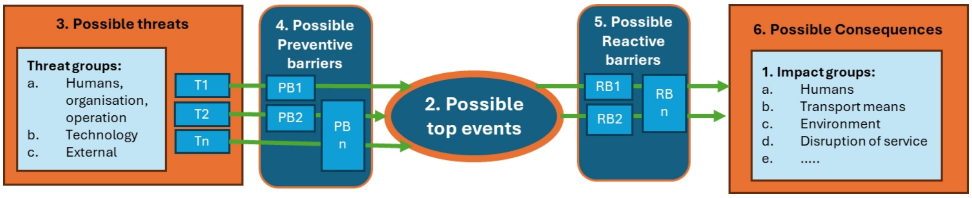


Figure 1: The resilience assessment methodology introduced in AEGIS, source: SINTEF.

- **Step 1:** Describe different impact categories as a contribution to defining the focus of the analysis.
- **Step 2:** Identify top events related to the consequences identified in step 1.
- **Step 3:** Through HAZID workshops, identify relevant threats as possible triggers for the top events in step 2.
- **Step 4:** Link the most critical sources of threats in step 3 to possible preventive barriers and measures.
- **Step 5:** Identify reactive barriers based on the top event and describe consequences if the barriers fail.
- **Step 6:** Identify worst case consequences from a top event.

The second step of the framework utilize the integrated planning for autonomous transport systems (IPA), as presented in Fjørtoft et al. (2023). Yet, this paper further details emerging issues related to human and technology interactions. This by presenting a method for how to secure resilience during the design, planning and follow-up of autonomous ship operations. Ultimately contributing to secure resilience into the transport operation.

Figure 2: The IPA planning levels, source: SINTEF.

The IPA methodology refers to four levels of planning: Strategic, tactical, operational, and executional, where the last one was introduced with the purpose of doing planning and decisions based on real-time data that also can be done by the technology (e.g. by means of Artificial Intelligence - AI). The suggested framework in this paper focuses on the tactical and operational levels but can in principle be applied also to the strategic and executional levels.

Why is there a particular focus on autonomy in transport systems? The answer is simple, yet complex: As an example, an autonomous vessels are likely to sail with different degrees of autonomy, depending on the ongoing operation and its surroundings. Described as operational envelopes in "Towards approval of autonomous ship systems by their operational envelope" (Rødseth, 2021), the overall operation must be broken down into sub-operations such as sailing in open seas, berthing, cargo loading/unloading (crane operation), etc. The level of human interaction in all these sub-operations may vary substantially depending on the level of autonomy and the number of vessels and/or equipment one human is responsible for.

The third and final step of the framework is based on the work of Hagaseth et al. (2023). In their paper, the authors studied how such operations can be described in a systematic and structured way. Figure 3 shows and suggests that these operations can be formalized by using UML[3] diagrams, as indicated to the right in the figure.

The methodology shown in Figure 3 starts with a textual and high-level description of the **Mission**, which in our case is the transshipment of containers from a daughter vessel to a mother vessel. The mission is further detailed into the **Context** (external actors), **Actors** (internal), **Ship particulars** (in our case the capabilities of the transport system), and the **Mission phases** (the different phases in the operation that can be described by a set of parameters, and further generalized into **Phase patterns**). The ship particulars form the basis for the description of the **processes** that the transport system components must be designed to handle. The **SCT** (System Control Task) describes the safe operation of each part of the transport system in a certain mission phase pattern. Of most relevance to our usage in the threats- and barriers analysis, is the various UML diagrams shown to the right in Figure 3. **UML use case diagrams** can be used to give a structured, high-level overview of the activities and the related actors, and to define the scope of the analysis. By adding the concept of misuse cases (Sindre, Opdahl, 2005), these diagrams can also be used to indicate top events (step 2), threat sources (step 3), and preventive and reactive barriers (step 4 and 5). The other types of diagrams can be used for further detailing of the results from the analysis: **Activity diagrams** describing the dependencies between activities are useful when more details are needed, compared to a use case diagram. **Collaboration diagrams** are useful when describing the hand-over between humans and automated systems, while **sequence diagrams** are useful for describing the communication between the different actors involved in the transport system, and possible attacked imposed on the communication. **UML state diagrams**

[3]Unified Modelling Language

can be used to give more details of each system's state, and this can be used in combination with collaboration diagrams.

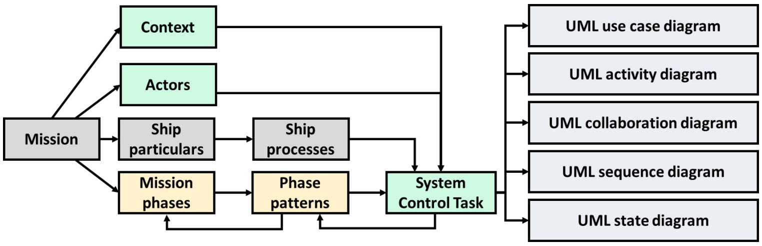


Figure 3: Analysis of MASS operation, source: Hagaseth et al. (2023).

The combined framework for assessing resilience in a maritime autonomous transport system thus consists of the three aforementioned methodologies and is exemplified through the following case study. This by combining research results from the MARMAN and the Horizon 2020 projects AUTOSHIP[4] and AEGIS. The latter is exploring the promising potential commonly associated with autonomous maritime transport, which is the realization of low- or unmanned mother (sailing ocean distances) and daughter (sailing local transport) vessels. Particular attention will be given to possible changes in roles and the sharing of functions between humans and technology.

EXEMPLIFIED USE OF THE FRAMEWORK

This section shows how the resilience framework described above can be applied on a simplified use case, and how UML modelling can be used to present the activities and events representing the threats and barriers identified through a risk analysis starting with the bow-tie-analysis as shown in Figure 1. The starting point for the use case is the transshipment of containers from a daughter vessel to a mother vessel. The daughter vessel is uncrewed, meaning that a Remote Operation Centre (ROC) is needed to monitor and control the operation of the vessel. The mother vessel has crew onboard. The mother vessel also has an autonomous crane onboard to load cargo from the quay side and onto the mother vessel, but this crane still needs supervision from onboard crew to handle exceptions during the operation. Since the terminal is designed to be highly automated, a Port Control Centre (PCC) is needed to do monitoring and control of the cargo flow through the terminal.

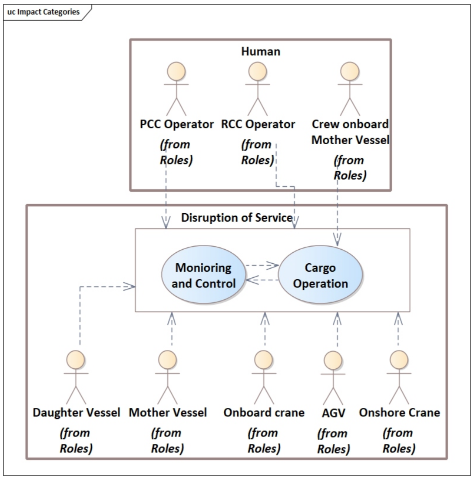
The case study is based on the AEGIS project, which investigated a transport system consisting of bigger continental container ships in combination with small autonomous feeder ships, remotely operated from a ROC, where one operator has the responsibility for several ships. The proposed framework is applied to a specific example herein where the three feeder ships are operated by one ROC operator.

[4]https://www.autoship-project.eu/

The mission is described by a set of mission phases that are generalized to a set of mission phase patterns (*Mission PhaseMission Phase Pattern*) as follows: (*Daughter vessel arrivalBerthing; Mother vessel arrival-Berthing; Unloading cargo from daughterCargo operation; Move container through terminalCargo operation, Load mother vesselCargo operation, Depart mother and daughterDeberthing)*. The following processes are selected for this brief use case description: **1**) Discharge of the daughter vessel by an autonomous crane on shore, **2**) Movement of the container by an autonomous vehicle to the quay where the mother vessel is moored, and **3**) Loading containers onboard the mother vessel using onboard cranes.

Further details on each steps taken during the analysis of this example, are shown in the following tables, where each step refers to the steps from Figure 1.

Step 1: Selection of impact category

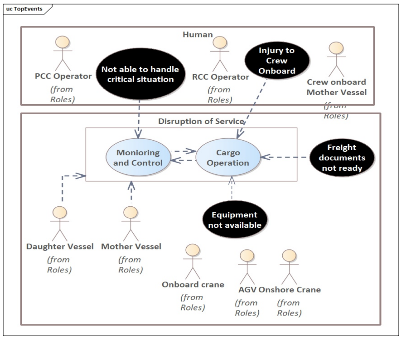


The first step is to consider the **impact category**, that is, who will be affected when an event occurs. An impact category, following the paper focus, refers to the consequences to humans, technology and reputation (regarding the transport service quality) when an event occurs. The first step in the methodology is to decide what category(ies) to focus on, to limit the scope. In this use case, we have selected the following two impact categories: ***Human:*** People onboard the mother vessel and operators in the Remote Control Centre (RCC) and Port Control Centre (PCC), ***Disruption of service:*** Technical failure of loading equipment or administrative issues during the operation.
The diagram shows the different users involved and their relation to each of the use cases. The light blue circles indicate use cases, and dependencies from each of the actors to the use cases are shown by dotted lines.

Describe worst case scenario for selected impact category

Impact categories	Description (Worst Case)
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.
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.

Step 2: Selection of Top Events

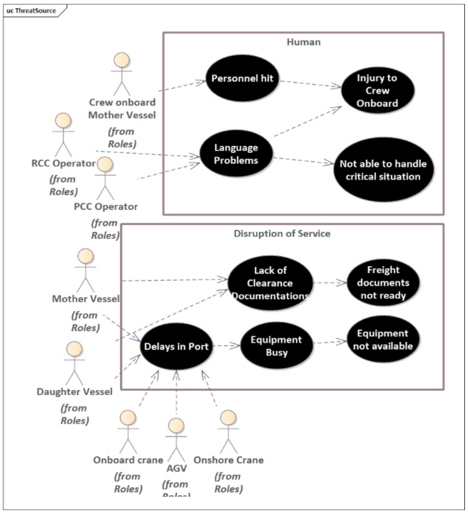


Identify possible top events relating to the impacts identified in step 1, forming the basis for further analyses. Examples of top events for the paper's use case are mostly related to the *impacts on personnel involved in the operation*, both the crew onboard and the operators in the RCC and PCC, and also to the *disruption of service that* can be damage to cargo or time deviation to transport. *As for our study purpose, the events could be:* Injury to crew onboard, Operators in the control centres not able to handle all critical situations, Freight documents not ready, Equipment not available, Discharging and loading equipment not available (Equipment failure or malfunction, failure in maintenance, or equipment busy with other loading tasks), Terminal tractor not available due to failure or is busy with other tasks. This diagram shows possible top events (black circles) and how they may relate to use cases (light blue circles) and the actors. The concept of misuse cases (Sindre, Opdahl, 2005) is used to model possible top events in a UML use case diagram.

Describe the main focus, the impact category, the top event, the likely reason for an event. (A database with event types is available)

	Top event (some examples)	Typical reasons for the event
Impact: Disruption of service **Main carriage:** Mother vessel	Cargo not ready for discharge or loading	Traffic jam outside the terminal; port congestion
	Loading equipment not available	Equipment failure or malfunction; Equipment faulty maintenance; Equipment busy with other loading tasks
	Freight documents/Clearance not ready	Delay of administrative/customs procedures
	Failure navigation/berthing/mooring equipment/sensor	Failure of equipment, No berth available
	Transport means not ready for loading	Failure of vehicle; vehicle busy with other tasks, Slow cargo operation, Bad weather, Lack of pilotage into port, Late arrival vessel

Step 3: Selection of Threat Sources



In step 3, sources of threats must be identified for each impact category and top event. In the example shown in the use case diagram to the left, we have selected the top events "Not able to handle critical situation" and "Injury to crew onboard" for the impact category "Human", and the top events "Freight documents not ready" and "Equipment not available" for the impact category "Disruption of Service". In the example case described in this paper, we have selected the following threat sources: **Human** (Language problem between the involved stakeholders and workers, Personnel hit by autonomous equipment), **Disruption of services** (Lack of documentation for cargo/load units to be transported (clearance, safety, insurance, etc), Equipment busy with cargo operations for another vessel that was delayed into port).

Decide the threats group to be used

Human, organizational, 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

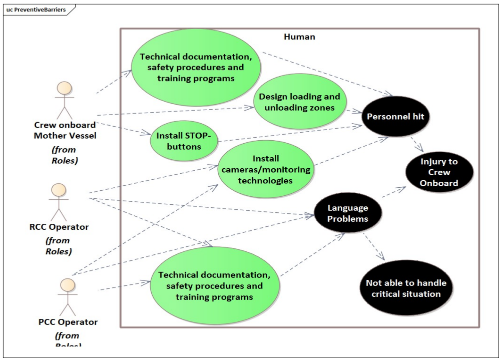
Technological sources of threats

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)

Step 4: Identification of Preventive Barriers and Measures



The next step is to identify preventive barriers and measures to reduce the likelihood of selected threats to happen. The aim is to link the most critical sources of threats to possible preventive barriers, forming the structure for developing preventive measures. Possible barriers related to this use case are shown in the UML activity diagram. The diagram shows the link between the identified sources of threats (black circles) and current barriers of a preventive nature (green circles) for the impacts on humans. Note that the overview must not be regarded as complete, but more as an example of the application of the framework.

Decide possible barriers to mitigate the selected threat group. Two examples are included here (Main threats identified and possible preventive barriers).

Human oriented: 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).

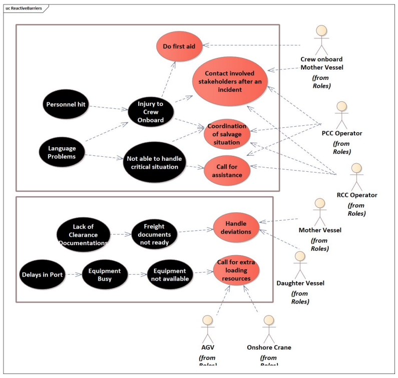
Implement E-learning or other training programs for workers and operators

Disruption oriented: 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.

Integrated planning and shared information between involved in the transport system

Steps 5 and 6: Identification of reactive barriers and measures, and consequences



Step 5 consists of identifying reactive barriers and measures to reduce the consequences of top events, after they have occurred. Step 6 describes possible consequences and negative outcomes of the top events that may occur if the preventive and reactive barriers fail to compensate for these effects. This step must be aligned with step 1, the impact group selected for the use case.

Some examples of reactive barriers are shown in the UML activity diagram. Red circles indicate reactive barriers, while the black circles indicate threats and top events. "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.

Decide possible barriers to mitigate the consequences. Some examples are included here (Collaboration, low planning quality, information exchange between parties/ICT-systems, procedures).

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.
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.
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.

CONCLUSION

The framework described in this paper highlights the importance of structuring the resilience assessment of an autonomous maritime transport system, by stepwise walking through possible unexpected and unknown events that may occur and to prepare for possible actions to take. The stepwise process, that considers possible impacts, events, threats, and suggests possible barriers to mitigate consequences, is an important exercise when new technology is introduced, such as autonomous vessels. This fosters the collaboration between technologies and humans, between organisations, and between the different stakeholders involved.

The paper recommends that the planning process starts at a strategic and tactical level. If a RCC operator does not have the vessel specific competence, this must be identified at a tactical level to ensure that sufficient knowledge is gained before starting operation. Further, an operator must be able to act when something unwanted occurs, which triggers a close interaction both with the technology onboard a vessel as well as between stakeholders involved. The UML way of describing the use cases formalises these processes and assists in coping with the event or unwanted situation.

In this paper, the different awareness categories humans, technology and external were exemplified by a use case covering transshipment between a daughter and mother vessel. The framework described the ability to assess and ensure resilience when planning operations in autonomous maritime transport systems, while considering the interaction between humans and technology, and how it can be modelled to understand the events, barriers, and potential consequences.

The framework combined results from the Norwegian project MARMAN and the EU projects AUTOSHIP and AEGIS.

ACKNOWLEDGMENT

The authors would like to acknowledge H2020 AEGIS under GA no 859992, H2020 AUTOSHIP under GA no 815012 and RCN MARMAN project no 324726.

REFERENCES

Fjørtoft, Kay, et al. (2023). Assessing the resilience of sustainable autonomous shipping: New methodology, challenges, opportunities, Cleaner Logistics and Supply Chain, Volume 9.

Hagaseth, Marianne, et al. (2023). Structured Description of Autonomous Inland Waterway Barge Operations, J. Phys.: Conf. Ser. 2618 012015

Honour, Eric C. (2006) “A Practical Program of Research to Measure Systems Engineering Return on Investment (SE-ROI)”, proceedings of the Sixteenth Annual Symposium of the International Council on Systems Engineering, Orlando, FL.

Kaber, David B. (2018). Issues in human-automation interaction modelling: Presumptive Aspects of Frameworks of Types and Levels of Automation. Journal of Cognitive Engineering and Decision Making, 12.

Taubman, Philip. (June 25, 2008) Top Engineers Shun Military; Concern Grow. The New York Times Website: https://www.nytimes.com/2008/06/25/us/25engineer.html

Sindre, Guttorm, Opdahl, Andreas L. (2005) Eliciting security requirements with misuse cases. Requirements Eng 10, 34–44 (2005). https://doi.org/10.1007/s00766-004-0194-4