Resilience in automated transport systems

Deliverable D2.5 - Version Final – 2022-11-30

Aegis

Advanced, Efficient and Green Intermodal Systems

http://aegis.autonomous-ship.org/

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement Nº 859992.

Document information

Title	**D2.5 Resilience in automated transport systems**
Classification	Public

Editors and main contributors	**Company**
Kay Fjørtoft (KF)	SO
Dag Atle Nesheim (DAN)	SO
Lars Andreas Lien Wennerberg (LALW)	SO
Harilaos N. Psaraftis (HNP)	DTU
Seyed Parsa Parvasi (SPP)	DTU

Rev.	**Who**	**Date**	**Comment**
0.1	KF	2022-01-12	Draft document structure
0.2	KF	2022-11-11	Document ready for internal review
Final	DAN/HNP/SPP	2022-11-30	Revised document after comments by Kalmar Final version for submission to EC

This publication has been provided by members of the AEGIS consortium and is intended as input to the discussions on and development of new automated and autonomous waterborne transport systems. The content of the publication has been reviewed by the AEGIS participants but does not necessarily represent the views held or expressed by any individual member of the AEGIS consortium.

While the information contained in the document is believed to be accurate, AEGIS participants make no warranty of any kind with regard to this material including, but not limited to the implied warranties of merchantability and fitness for a particular purpose. None of AEGIS participants, their officers, employees, or agents shall be responsible, liable in negligence, or otherwise howsoever in respect of any inaccuracy or omission herein. Without derogating from the generality of the foregoing neither of AEGIS participants, their officers, employees, or agents shall be liable for any direct, indirect, or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

The material in this publication can be reproduced provided that a proper reference is made to the title of this publication and to the AEGIS project (http://aegis.autonomous-ship.org/).

Table of contents

Executive Summary

AEGIS is a next generation short sea shipping logistics concept that is currently under development. The objective is to solve some of the challenges faced by today's short sea shipping and maritime transport. This document, *D2.5 Resilience in automated transport systems*, is part of the AEGIS project work package 2, *Logistics system redesign and resilience*. This WP develops new methods for design of logistics systems for highly automated waterborne transport systems, where the method described in this report can be used to identify threats and possible barriers to be implemented with the ambition of reducing the consequences of an event. The whole work package objective is to emphasises possibilities inherent in autonomous ships, such as the possibilities for scaling down ship sizes to increase frequency and differentiate speeds, the use of more standardized cargo units and fully automated cargo handling in small and medium ports as well in transhipment terminals. The issue of cargo clearance (customs, phytosanitary, ISPS etc.) is also an important consideration, in particular for automation of work processes. Most of the actual redesign is done in the use cases (WP8 to WP10), but WP2 will provide tools and methods for analysing effects of redesigns and provide guidance for the process.

The outcome of the work with resilience in automated transport systems is a methodology for assessing resilience in transport systems. The objective with this AEGIS resilience methodology is to identify possible top events in the transport system, to prepare preventive and reactive barriers to the event with the purpose of reducing consequences. One way of working to consider new technology to be used in the transport system, such as autonomy or an autonomous vessel, is to identify challenges that might pose a threat when introducing it. These can be challenges that occur from different perspectives, that could be the human or organisational perspective, operational, as well as from a technological point of view. This report describes some possible top events and threats, as well as barriers that could be implemented to reduce the consequences of such events. The different steps are better explained later in this report, and at the end of the report there are a list of possible threats, barriers and measures that can be used as a check list when working with the methodology. It is likely that new issues will be introduced when working with a specific use case.

Definitions and abbreviations

AIS: Automatic Identification System

DC: Dry Storage Container

DFDS: Det Forenede Dampskibs-Selskab

EPS: Expanded polyester boxes

FEU: Forty feet equivalent unit

GC: Grieg Connect

GT: Gross Tonnage

HC: High Cube container

ICT: Information and Communication Technology

IMO: The International Maritime Organization

ISPS: International Ship and Port Facilities Security Code

ITS: Intelligent Transport System

LBG: Liquefied Bio Gas

LNG: Liquefied Natural Gas

LoLo: Load on Load off

MASS: Maritime Autonomous Surface Ship

MGO: Marine Gas Oil

NCL: North Sea Container Line

NTP: National Transport Plan

PTI: Pre-Trip Inspection

RoLo: Roll on Lift off

RoRo: Roll on Roll off

ROC: Remote Operations Centre

SO: SINTEF Ocean

TEU: Twenty feet equivalent unit

TRH: Trondheim Havn

WP: Work Package

1 Introduction

1.1 Objective

This document, D2.5 is a deliverable in work package 2 and the objectives of this document are given in the Task 2.4 description:

D2.5: Resilience in automated transport systems (PU, DTU, M30)

Task 2.4: Resilience in automated transport systems (DTU, SO, DFDS, NCL – M12 to M30). *This task will investigate and quantify improvements of transport system resilience after the redesign has been made. This will be an incremental process where initial outputs from this task will, if necessary, be used to modify the new transport systems. The theory is that a system with more and smaller ships will provide a system with higher resilience against disruptions, being it due to environmental issues (worsening climate), technical (defects in a ship or terminal equipment) or hostile physical or cyber-attacks. Part of this is also LOLO versus RORO cargo on the different ship types. In principle, the analysis tools developed in WP5 could be useful in this task, but this will also be investigated.*

It must be clarified right at the outset that, for reasons related to progress in other AEGIS work packages, and in a strict sense, a "quantification" of transport system resilience after the redesign has been made, has proven not possible within the context of the present deliverable. Such a quantification would have to be linked to the three use cases:

- Use case A: *Short sea and terminals in Norway*
- Use case B: *Short sea and inland interface in Belgium and Netherlands*
- Use case C: *Revitalizing regional ports and city centre terminals*

This report presents a methodology for investigating resilience in a transport system. Redesigned logistics systems are case specific, and it is suggested that resilience investigations are included as part of the upcoming deliverables in the use cases, specifically for use case A and B, within the deliverables *Detailing and validation of use case A* and similar for *B (D8.4 and D9.4)*. Since this report is part of WP2 and on a generic level for logistics systems it was concluded that the content should also be.

Resilience and recovery KPIs have been defined in the context of Task 7.1 (see deliverable *D7.2 Report on KPIs* [6]), however the quantification of such KPIs is still pending as it depends on data that has proven still not available.

We also note that the importance of bottlenecks and obstacles in overall system performance in use cases A and B (both for the "baseline" non-AEGIS solution and for the AEGIS solution) can be found in deliverables *D8.3 Bottlenecks and obstacles in Case A* [7] and *D9.3 Bottlenecks and obstacles in Case B [8]*, respectively. The reader is referred to these deliverables. These were being finalized in parallel with this document. This can be helpful in assessing the potential improvement of the AEGIS solution vs the non-AEGIS baseline solution. A specific example on use case A is presented in this deliverable, however the analysis is not quantitative.

1.2 Background

Autonomous shipping is enabled by several emerging technologies, like advanced sensors, machine learning, Artificial Intelligence, and improved connectivity (Internet of Things), and by using the digital infrastructure in a more advanced way than conventionally. Autonomous shipping also requires interaction between technology and different stakeholders and organisations along a value chain, for example with a (remote) control centre to operate a vessel. It is important to focus not only on one single node in the chain, but also the interaction with the other nodes/stakeholders. For instance, a reach stacker at a terminal will be feeding cargo between vessels and trucks, as well as to the depot in the terminal. This example demonstrates that the reach stacker in one way or another must exchange data with at least three different ICT systems or organisations, 1) the vessel operator, 2) the truck operator, 3) the terminal system.

For example, Onishchenko et al. (2022) [1] studied cyber resilience of ship information systems. They declared that the increasing use of remotely controlled autonomous ships today leads to an increase in new types of cyberattacks worldwide as well. Hence, they developed a basic response plan to protect ship control systems by analysing the cyber incidents. Also, their initial response plan is updated regarding the new conditions.

Wang et al. (2019) [5] examined the resilience perspective on sea transport mode in the Eastern star case. The Eastern star is a cruise vessel that travels along the Yangtze River, including a tour of the three gorges. They focused on two types of accidents that come from natural and human-induced causes. They tried to improve safety based on comprehensive risk assessment at the theoretical and operational levels concerning the specificities of water transport.

When working with resilience it will be important to understand possible events that can happen, the threats along the transport chain and in the transport system (see Figure 1), to identify barriers, and to plan for actions if something happens or stops. Resilience is also to prepare for the unknown and to be able to act on the unknown. It is of high value that there are systems, procedures, or plans, to be used to minimize consequences of an event. In AEGIS there is a particular focus on how to implement more automation and autonomy into the transport system. It is of importance to plan for the unknown, what can happen and how to come back to normal if something fails or stops.

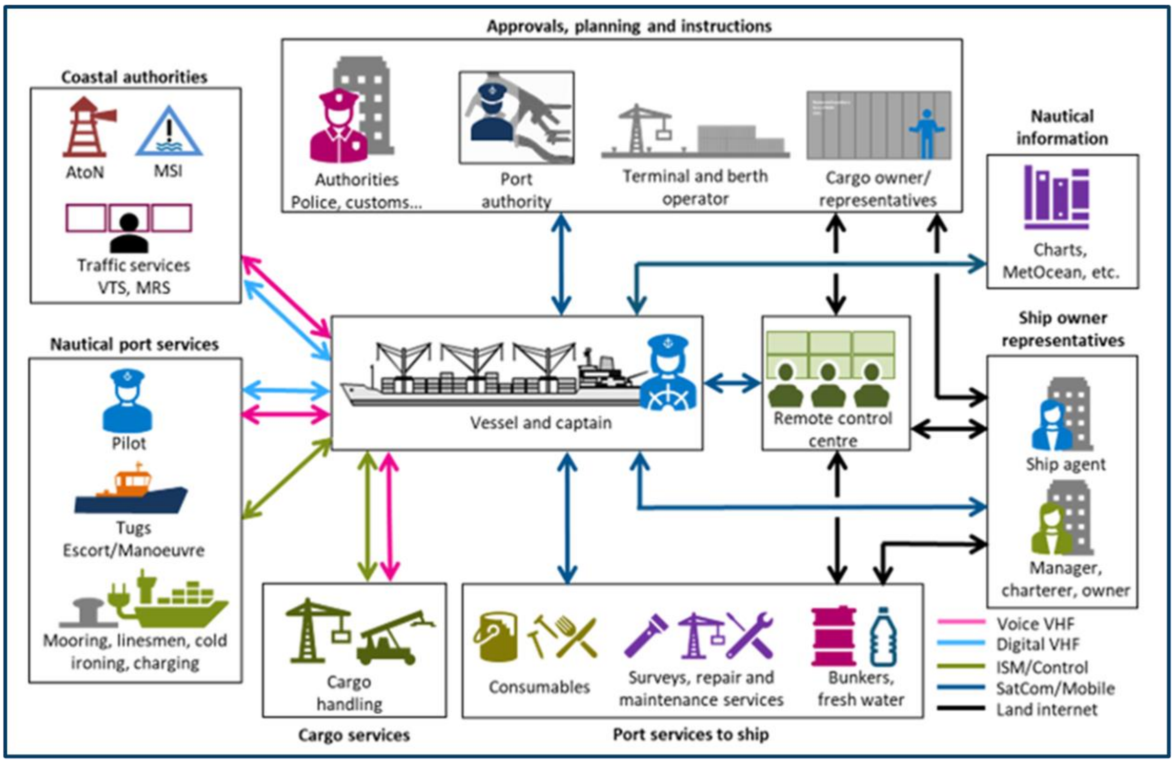

Figure 1: The overall Ship transport system

1.3 Examples of use of autonomy

Due to legislation reasons, the development of autonomous technology for the shipping sector will follow different degrees of autonomy.

The International Maritime Organization (IMO) have pointed to following degrees of autonomy[1] when focusing on vessel operations, a similar degree level can also be implemented for crane operations or trucks operating in a terminal area:

1. **Degree One: Ship with automated processes and decision support:** Seafarers are on board to operate and control shipboard systems and functions. Some operations may be automated and at times be unsupervised but with seafarers on board ready to take control.
2. **Degree Two: Remotely controlled ship with seafarers on board:** The ship is controlled and operated from another location. Seafarers are available on board to take control and to operate the shipboard systems and functions.
3. **Degree Three: Remotely controlled ship without seafarers on board:** The ship is controlled and operated from another location. There are no seafarers on board.
4. **Degree Four: Fully autonomous ship:** The operating system of the ship is able to make decisions and determine actions by itself.

The technology is in many cases ready for degree four, but the legislation is not ready to allow a fully autonomous ship without crew onboard. This is one of the reasons why many of the ongoing autonomous projects will firstly have crew available onboard the vessels, where the next plans will be to have a remote operation period before a fully computer-controlled voyage can take place (with or

[1] IMO - MSC.1/Circ.1638 3 June 2021 - OUTCOME OF THE REGULATORY SCOPING EXERCISE FOR THE USE OF MARITIME AUTONOMOUS SURFACE SHIPS (MASS)

without a remote backup for exceptional situations). The development of Yara Birkeland will follow this approach as an example. Current status of Yara Birkeland is that it is sailing in a test period, with an autonomy degree 1 and partly 2. It is expected that the different steps will identify needs for new technology, but we also expect that new resilience needs will be identified.

When working with a transport chain it can be important to identify some areas where the autonomy can be used. As example from Figure 2, the areas of interest could be a control room that should operate an autonomous technology, a vessel or crane to be operated, sensors onboard the vessel such as the possibility to monitoring an engine, the mooring or berthing system, the interaction with a tug or a reach stacker at a terminal. This is only examples that can be change with other technologies and operation areas.

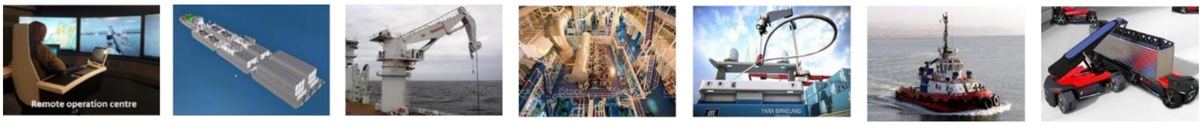

Figure 2: Types of autonomy

Figure 3 shows types of technology that could be involved in the various operations, where interaction is important for success. For example, the operation "*navigation*" will in most cases require that a vessel must be connected closely to a remote operation centre (ROC), which, based on its degree of autonomy must know its operational tasks. Such tasks could be whether the ROC should monitor the vessel or whether they should be able to actively operate the vessel if necessary. The tasks will be different depending on the level of autonomy that is introduced.

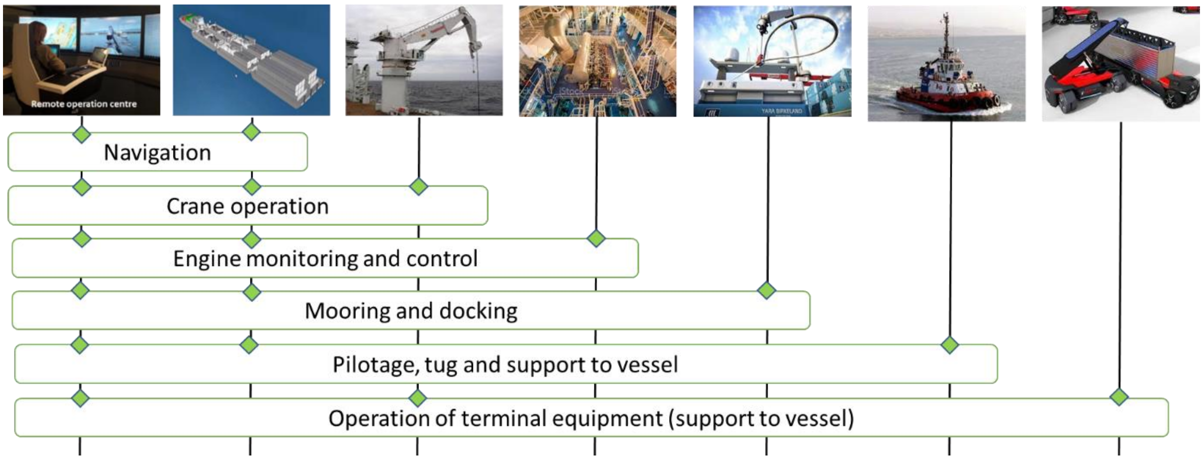
Remote operation centre
YARA BIRKELAND
Navigation
Crane operation
Engine monitoring and control
Mooring and docking
Pilotage, tug and support to vessel
Operation of terminal equipment (support to vessel)

Figure 3: Types of operations

1.4 Resilience

In autonomous systems it will be important to build resilience into the system where operational or technological limitations are identified and where safety and criticality should be assessed.

Resilience addresses the ability of systems, organisations and society to continue operations both under expected and unexpected situations (adapted from Hollnagel[2]). This is a response to the increased of complexity, interdependencies across critical infrastructures and uncertainty posed by the emergence of disruptive technological innovations, climate change and changes in geopolitical structures. Resilience is a transdisciplinary area of research that integrates social (e.g. sociology, psychology), formal (e.g. computer sciences) and applied sciences (e.g. engineering and technology). AEGIS will work with the application arena maritime transport, where communication, safety and cybersecurity, autonomy and digitalization within the transport system will be prioritised.

Introducing new technology like autonomous ships will change the way of working. To handle new threats, unfamiliar events, and incident types, planning and management should develop and rely on preventive measures. New indicators are needed in addition to the traditional, including foresight indicators handling both foreseen and unforeseen events, (Stene (2020) [3]. To address technological issues, it is important to build robustness and redundancy or to introduce options to recover from an unwanted situation. Regarding operational knowledge it will be important to understand the human's role, and how to utilize the human expertise in decision making. This is relevant when moving the operation from a traditional captain on board a vessel to a shore control centre. The shore captain will likely be responsible for navigating several vessels in parallel, which is a completely new scenario compared to today's practices from conventional shipping where the captain's operational domain is limited to one ship only. A shore-based captain is not always the best decision maker if the situation requires knowledge other than from the navigational field, for example if technological failures occur this will require an engineer's knowledge. An engineer will need different information for decision support than a captain. The main philosophy will be that the technology will be capable of making decisions on its own, but there will be situations where the technology will need human intervention and expertise in the sense- and decision-making process. Sense making means that reality is an ongoing accomplishment that emerges from efforts to create order and make retrospective sense of what occurs', Weick (1993) [4].

The understanding of the resilience is to have the ability to maintain essential system functions prior, during and after changes in the operational environment.

- ***Rebound*** – the ability to bounce back to stable state, the ability to recover from a disruption or surprises. In autonomous systems it can first move to a minimum risk condition before the situation is back to normal and ends up in a normal state. This will be to rebound or recover from an abnormal to a planned or normal state. This can for example be done with proper procedures or technical systems that can change states.
- ***Robustness*** – ability to withstand, to increased capabilities to absorb distresses. In autonomous solutions this can be to have redundancies to system as example. The systems must be able to adjust its behaviours to unforeseen situations. This can be technically, organisational, or to external factors where robustness could be introduced. To build barriers to withstand threats that can lead to an unwanted event, is an example of building robustness to the system.
- **Opposite of brittleness** – capacity to stretch beyond performance limitations. It describes how to cover adaptive ability regards surprises. It describes how a system extends performance, or brings extra capacity to tolerate unforeseen events that challenges its boundaries. It

[2] https://erikhollnagel.com/ideas/resilience-engineering.html

describes the degradation of performance that might occurs when the system pushes its boundaries beyond boundaries.

- **Network architecture** – ability to anticipate and adapt to changes and to future surprises, this when condition evolves.

Resilience can also be categorized into different levels or perspectives, namely global, regional, and local.

1. **Global perspective:** Often based on the world situation, such as war and major accidents or transport blockage of the Suez channel as examples. The impact in this category will be significant for the continents, countries, or societies and not only for one company or one trade. Often the threat can be materialized by political disagreements influencing the market balance, political balance, or trade balance as examples. The global perspective also entails happenings such as the Covid pandemic, lack of international infrastructure and main hubs (e.g., Port of Rotterdam) or lack of energy, or it can be environmental issues influencing a trade area such as low water in the rivers or ice problems in the northern shipping corridor. This perspective is somewhat out of the AEGIS project's main focus regarding implementation of barriers. Still, it can be of value to plan for a higher resilience level based on the global threats, but the mitigation measures should be implemented on a lower level.
2. **Regional perspective:** This level focuses more on a national and regional perspective. The decision makers (such as national government, municipal authorities, or regulators) have the power to regulate parts of the transport system and corridors. Examples of potential threat sources are local strikes and local activities, regional accidents that stops the transport in/out of a region. Regarding possible resilience measures, the community in the region should think about alternatives if corridors, ports, or terminals are not available for a period of time.
3. **Local perspective:** This perspective focuses more on a transport provider's level, the cargo owners, and the terminals as service providers in a transport system. Failures in loading equipment, lack of resources for load handling, and cyber-attacks are examples of threats within this category. In AEGIS this level will be of high importance as this is where there is most room for affecting the resilience in terms of concrete preventive and reactive barriers. This also counts for resources available, such as cranes or loading equipment that can be hired if something stops or breaks down.

1.5 Formal Safety Assessment

The above methodological framework clearly parallels the so-called Formal Safety Assessment (FSA) framework used by the International Maritime Organization (IMO) to assess risk in maritime operations, as well as choose the best way to mitigate such risk. FSA is typically applied to maritime safety problems, even though it has also been extended to environmental issues. See Psaraftis (2012) [2] for an overview of the method.

Specifically, IMO's Guidelines on the application of FSA recommend a five-step approach, consisting of the following steps:

1. Hazard Identification
2. Risk Assessment

3. Risk Control Options
4. Cost-benefit Assessment
5. Recommendations for decision making

An illustrative representation of this framework is given Figure 4 which was presented by the International Association of Classification Societies (IACS) at the 75th session of IMO's Maritime Safety Committee (MSC 75) in 2002:

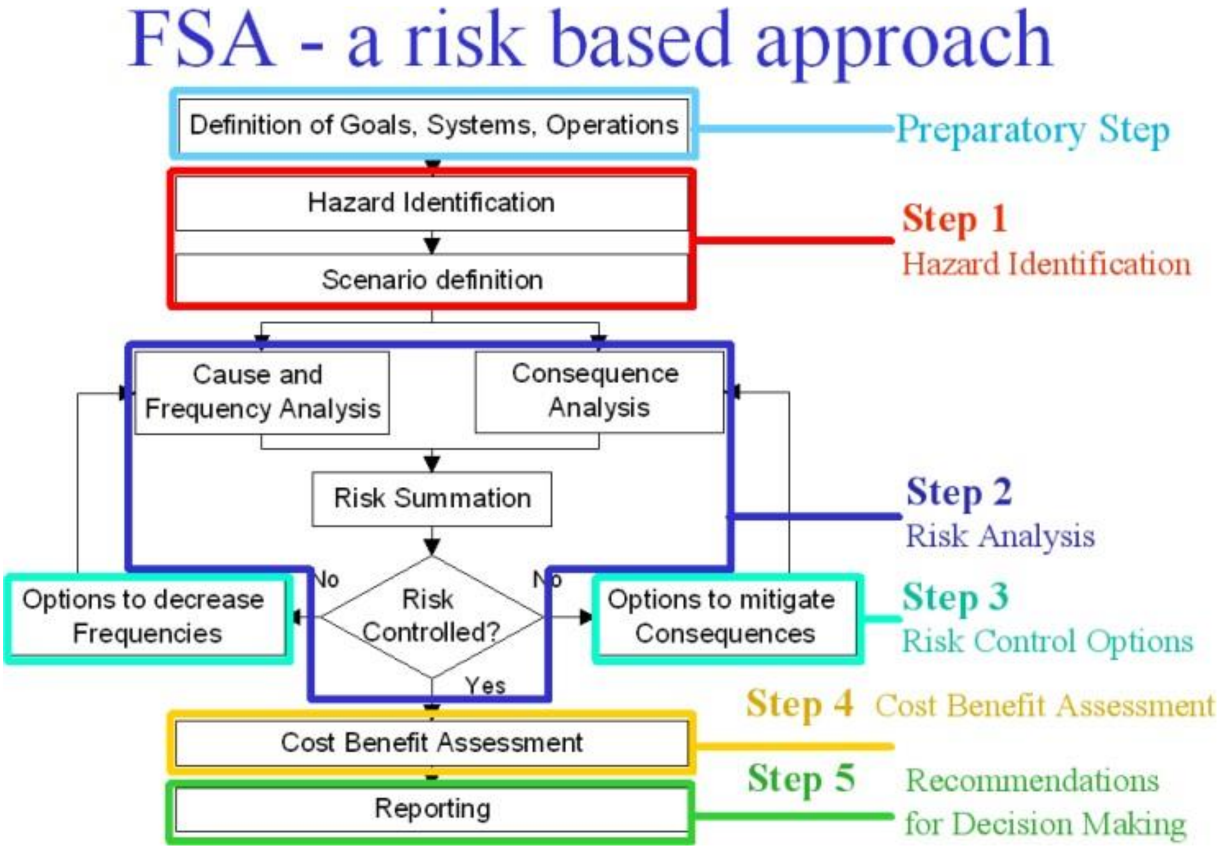

Figure 4: FSA Flowchart. Source: IACS

Even though there is no one-to-one mapping among the steps of the two procedures, there is a clear equivalence between Steps 1 and 2 of the FSA and Steps 1, 2 and 3 of the AEGIS approach. Step 3 of the FSA corresponds to Steps 4 and 5 of the AEGIS approach. In the AEGIS resilience assessment framework, we do not include Cost Benefit Assessment, nor Recommendations for Decision Making (step 4 and 5 in the FSA) but these would be natural next steps once the resilience assessment has been concluded and the results from the resilience assessment would be very useful for this.

2 AEGIS Resilience Methodology

When assessing the reliability of a logistic chain, one need to consider a number of different operations, performed with a number of different stakeholders involved in a transport system taking into account a number of different threats, unwanted events, potential consequences, and measures for mitigating either the probability of unwanted events or the consequences of unwanted events. These can later be organised into bow-tie diagrams, visualising the probability and consequences of unwanted events, affecting the resilience of the logistic chain. Bowtie is a well-known method and structured approach for identifying and visualizing safety-related barriers and measures. Both in relation to preventive (probability-reducing) and reactive (consequence-reducing) identification of barriers. Figure 5 shows the bow-tie diagram as used, where the left side shows sources of threats that can trigger a given top event (in the middle of the diagram), and the right-side possible consequences of the top event that occurred. All the consequences can be said to represent a spectrum of consequences. The arrows symbolize the connection between the respective sources of threats via the triggered top event and possible consequences. These are interrupted by potential barriers or measures to reduce the likelihood (green) of a top event actually occurring or reduce unwanted consequences (orange).

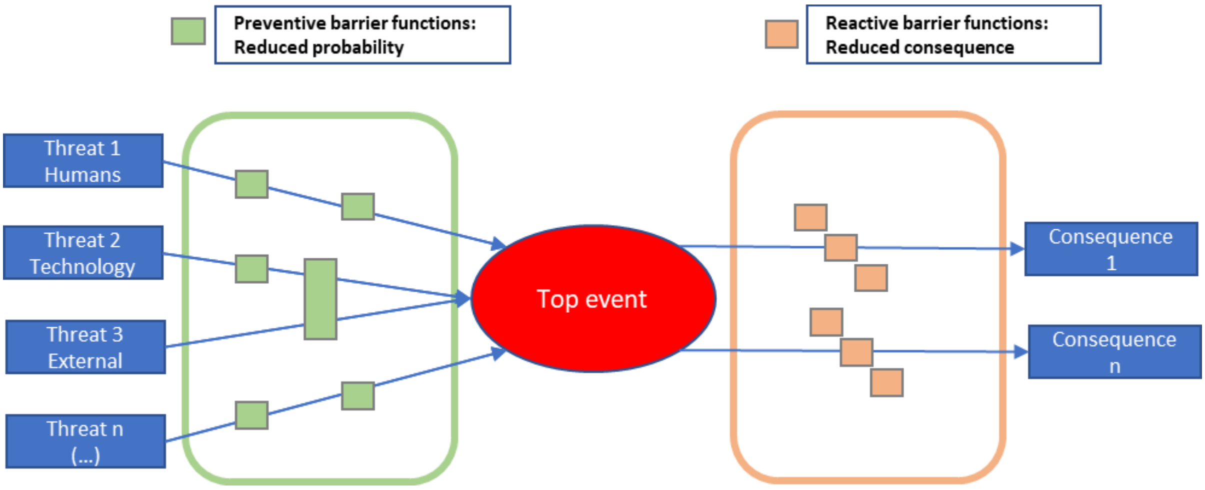

Figure 5: Generic bow-tie diagram

Before identifying the potential unwanted events, the associated threats and preventive mitigation measures, the potential consequences and reactive mitigation measures, one need to consider the operations for which one wants to assess the resilience. For logistics chains, there are different alternatives one may consider the overall resilience related to transporting goods from a point of origin to a final destination. In many cases, this is what the cargo owner cares about. The transport system itself is more of a black box. Four our purpose, the more suitable alternative is to look at each individual node and leg in the logistic chain, practically opening up the black box and have a look inside (see Figure 6)

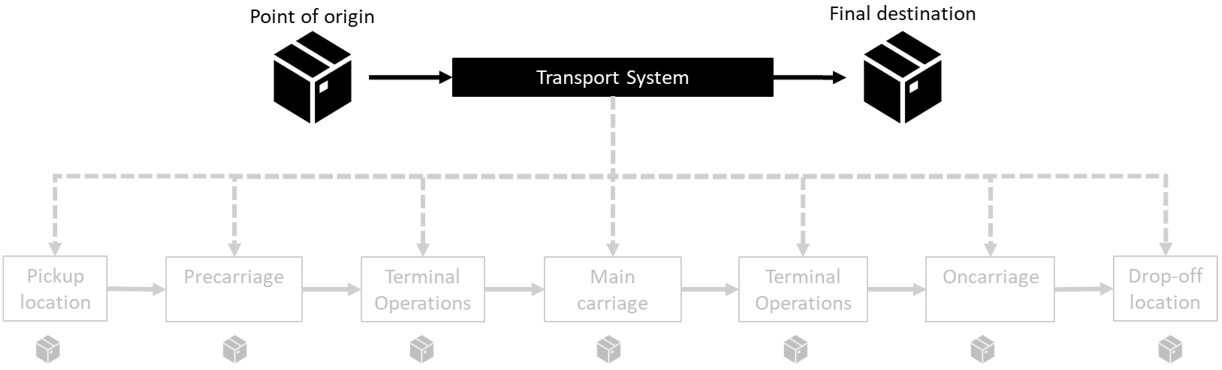

Figure 6: The transport system as a black or white box

The reason is twofold: We want to assess the reliability of the processes (operational, physical and/or digital) which constitutes the overall logistic chain, and we want to identify measures/barriers for improving resilience which can be implemented by the individual stakeholders in the logistic chain. This become more evident when we start identifying unwanted events and how to deal with them (see Sections 2.1.2 and 6.2.2).

The framework to be used in AEGIS is regarded as generic, and thus also of value for the development of solutions that go beyond the project's main focus - namely the development of solutions that can be used when abnormal event occurs. The framework consists of six different steps (see Figure 7):

- **Step 1:** Description of different impact categories as a contribution to defining the focus of the analysis.
- **Step 2:** Identification of various top events related to the consequence (s) identified in point 1, and thus the basis for further analyses.
- **Step 3:** Through HAZID workshops, relevant sources of threats are identified that can occur, and which can thus trigger one or more of the selected top events in the bow-tie diagram.
- **Step 4:** The sources of threats that are considered most critical are linked to possible preventive barriers and measures. These forms the basis for further work with a view to developing preventive measures.
- **Step 5:** Based on the top event that has occurred, possible reactive barriers are identified, as well as a description of various consequences if the barriers fail.
- **Step 6:** Identify possible worst consequences of a top event

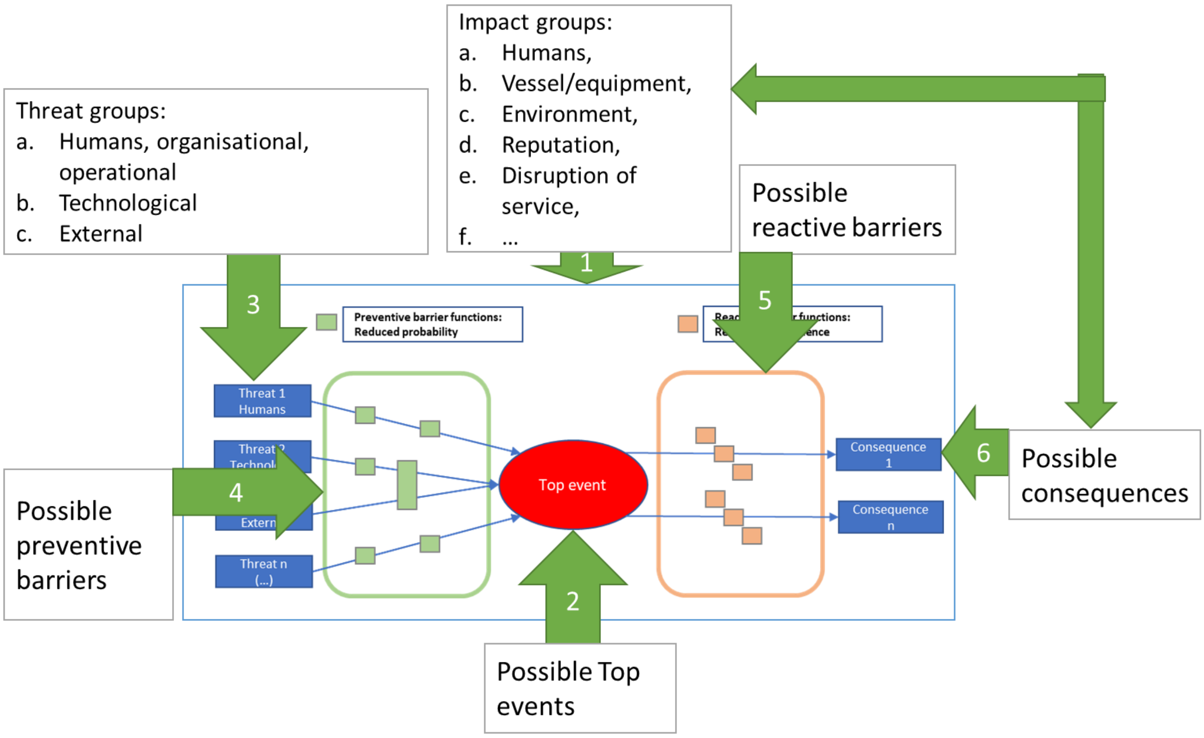

Figure 7: Steps in the AEGIS Resilience methodology

The framework is based on the following definitions:

• Impact categories are the losses that can occur if a top event occurs, for example that transport means are lost. The impact categories and priorities between these can potentially differ from user case to user case, but also from analysis to analysis.

• Top event is the event that can occur and which in the worst case can trigger unwanted outcomes that are listed as consequences.

• Sources that describe various threats that can trigger a top event. Different sources of threats can lead to the same top event.

The framework for the implementation of top events and identification of threats can be developed on the basis of workshops organized by the AEGIS Use-cases. The methods used in the various steps are summarized in separate subchapters. The workshops formed the basis for identifying the most relevant sources of threats and top events. The visualization supported the identification of barriers and measures that contribute to reducing the probability and consequences of the respective top events. The results from this work, supported by discussions with project partners, formed the basis for establishing the framework itself.

2.1 The different AEGIS Steps

Possible top events, threats, and barriers which was used and validated in workshops on resilience for AEGIS Use Case A. This chapter introduces a limited list, a list which might be changed and new items can be added. The list is meant as input to a workshop, from where new items will be included.

2.1.1 Step 1: Identification of impact categories

The choice of relevant impact categories is important for the identification of relevant top events, but also creates a common understanding of which focus should be leading for the analysis. The impact categories must be determined before the analysis, so that the assessment takes place in a consistent and uniform manner. The impact categories can affect humans/people, technology, equipment and infrastructure, environment, and reputation, as well as disruption of services, as shown in Table 1. In the AEGIS use cases the "disruption of services" will be of highest interest, but also to understand the impact of introducing automation or autonomy to the transport system can be of relevance.

Table 1: Impact categories

Impact categories	Description
Humans	The risk consists of human lives being lost or people being injured. People include passengers, workers on board vessels and terminal, crew on board, drivers, personnel assisting in logistic operations or other people who in one way or another come into contact with the transport chain. It may be relevant to use different degrees of severity that are expected, for example, loss of several lives, loss of a life, serious injury to one or more people, minor injury to one person and so on.
Vessel, equipment, and infrastructure	The risk consists of the vessel and / or terminal equipment being lost or damaged. Expected extent of damage can be measured differently, for example through expected loss of monetary value. Grading losses can be useful in comparing consequences as a result of different sources of threats.
Environment	The risk consists of an incident causing damage to the surrounding environment (other road users/ vessel/quays, etc.), or the environment through discharges. Risk can be described through expected damage / destruction and can be expressed through monetary value.
Reputation	The risk consists of an incident occurring affecting the reputation of the operator and/or the operation of i.e., autonomous ships in a negative sense. Thus, affected by the severity of the mentioned impact categories (human, vessel and infrastructure, environment).
Disruption of Service	Any disruption of the transport chain, resulting in unexpected delays or damage to- or loss of cargo. Disruption could be a result from technical failures, operational or administrative issues, or could also be a result of external factors such as bad weather that leads to deviations.

2.1.2 Step 2: Selection of top events

Based on workshops, and with other input from the industry and available literature, the project should identify different events that are considered most critical in order to ensure an adequate level of logistics performance, that for some cases also includes operational safety within the transport chain. Prioritization of the top events listed in Table 2 is based on the use cases and based on experiences that the project group has in accordance with a transport system where inland waterways transport and short-sea shipping operations and terminal activities are of high interest. When applying the framework to other use cases, or other focus areas, other top events than those listed as examples may be more relevant.

Table 2: Top event (example related to transport of cargo and ***disruption of services****, ref figure 4 and table 1)*

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 No berth available

	4.5 Transport means not ready for loading	Failure of vehicle; vehicle busy with other tasks Slow cargo operation Bad weather Lack of pilotage in to port Late arrived 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 Lack of labour 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

It is likely to work with step 6 in the context of step 1 and 2. The consequences will be a factor of the selected top events to be reviewed. The reactive barriers are used to reduce the consequences, which is part of the step 5 work.

2.1.3 Step 3: Selection of threats sources

Based on defined top events, threats sources are identified in step 3 from three main groups (Table 3); i) Human, organizational, operational threats, ii) Technological threats, and iii) External threats. These in turn have different subgroups to facilitate as concrete and specified an analysis as possible.

- The threats source groups i) and ii) entail conditions and events that one can do something with, something that can be controlled through design, procedures, etc.
- Threats source group iii) entails threats of such a nature that they are often uncontrollable, such as environmental forces in the form of waves, wind, currents, tides, river water level, etc.

The identified sources of threats are described in chapter 3. Some of the subgroups focus on operational conditions, while others are more technologically oriented. These are intended as support to identify threats that are relevant to a selected event. Therefore, it is necessary that the sources of threats described in the document are adapted to the threat's scenario for analysis (i.e., connection between top event, user case and consequence categories). The identified sources of threats form the basis for step 4 (identification of preventive barriers).

Table 3: Sources of threats

#	Sources of threats
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)

2.1.4 Step 4: Identification of preventive barriers and measures

Step 4 of the framework deals with the identification of possible preventive barriers and measures (i.e., probability reduction), and is on the left side of the bow-tie diagram. The diagram is a good tool in such a process, as it communicates well and contributes to good discussions. In support of the identification of possible barriers and measures, the main goal will be to establish an overview. The choice of relevant barriers and measures is based on the relevant and most critical sources of threats identified in step 3 (see also detailed overview of identified hazards). The work will be as follows:

1. Area of interest, see Table 3
2. Identify and select threats to be investigated, see Excel sheet
3. Identify and select preventive barriers, see Excel sheet

Critical sources of threats are understood in this context as the threats that, according to the project's assessments, can occur with high probability, but also the threats where the undesirable consequence is as highest. The work shows how different threats relate to the 3 three main groups, Group 1: Human, organizational, operational sources of threats, Group 2: Technical sources of threats, Group 3: External sources of threats, but also the connection between the various threats and current preventive barriers. The latter are measures that are considered to actually contribute to reducing the probability of a top event occurring. Chapter 4 describes possible preventive barriers and measures in more detail but note that these must be adapted to the user cases and threats scenario (top event and focus) that is analysed.

It is important to note that when describing barriers and measures, the design criteria for these are also described. In the form of RRF (risk reducing factor), one describes how effective a solution should be and thus reduces the probability of an undesirable event occurring (i.e., the top event). SIL (Safety

Integrity Level) focuses on safety, reliability, and the quality of the barrier/measure. Both RFF and SIL are not discussed in more detail in that context.

2.1.5 Step 5: Identification of reactive barriers and measures

Corresponding to step 4, step 5 selects which reactive barriers and measures are to protect against undesirable consequences given that a top event has occurred (e.g., crane failure). These are located on the right side of the bow-tie chart. The work will be in a similar form as for step 4, but with reactive barriers as focus, and the defined main categories of different sources of threats are also used here to structure and document the connection between source of threats, threats and consequence-reducing measures and barriers.

2.1.6 Step 6: Identify possible consequences

The various categories must be considered as factors that can influence the course of events, and how to reduce the effect of influence from these. With "Reactive barriers" you note barriers and measures that will reduce the effect of an unwanted top event. With "Consequence", possible outcomes are noted if various barriers are broken, or measures do not stretch. It is therefore a strong connection between the top events defined in Step 1 with the consequences identified, which means what will be the worst case if it will not be possible to stop the escalation of a top event. The list of relevant consequences is intended for use when defining the right side of the bow-tie diagram, in following chapters a list of a number of impact reduction measures that can be helpful in identifying more specific barriers and measures.

3 Threat sources

Based on the results from previous projects and internal workshops in AEGIS, the identified sources of threats were organized into different groups and subgroups (as described previously), and this chapter provides a detailed description of each of these. The chapter thus provides useful guidance when relevant treats on transport resilience are to be identified and documented. The content also forms an important starting point for identifying relevant probability-reducing measures and barriers. It is emphasized that the documented threats for each individual source of threats represent transport in general and are not intended to be exhaustive. This is because threats will vary from user case to user case (e.g., length of route, location, speed range, degree of autonomy, technology in use, etc.).

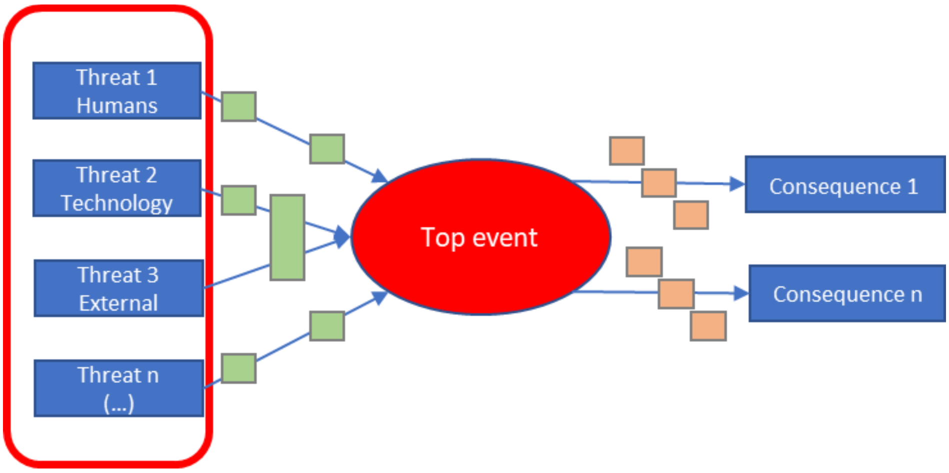

Figure 8: Identification of Threats

3.1 Human, organizational, and operational sources of threats

The subgroups organized under the threats source group 1, Human, organizational and operational threats sources are:

(1) Terminal workers and crew, external service providers, operation centre and

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

3.1.1 Threats sources Terminal workers and crew, external service providers, terminal workers, operation centre

This source group deals with threats that may arise due to human limitations or failures, incorrect or defective procedures, or operational limitation because of organisational boarders, as can be seen in Table 4. These can occur on board the vessel during crossing, as well as during boarding and disembarking, as well as at a terminal when loading or unloading activities happens.

Table 4: Threats sources passengers, crew, and terminal workers

#	Threats sources Terminal workers and crew, external service providers, operation centre
1.1	Crew and terminal workers with unforeseen medical needs (cardiac arrest, malaise, seizures, and loss of consciousness, etc.).
1.2	Crew and terminal with unintentional or erratic behaviour – acting out and/or under the influence of drugs.
1.3	Crew and terminal workers with inadequate ability to handle.
1.4	Crew, drivers, and terminal workers in shock and/or with an irrational reaction pattern (e.g., in the event of an accident, stress).
1.5	Accidents within the transport systems, as example crew falls into the water at the quay side ("Man overboard" observed and not observed).
1.6	Crushing injuries for crew and terminal workers (especially boarding and alighting).
1.7	Lack of control over the number of people at the terminal area or on board the loading zone at a vessel.
1.8	Stress due to low staffing, crews/terminal workers have too many tasks that must be handled in parallel.
1.9	Lack of control over what crew/workers carry on board which can be threat source.
1.10	Lack of competence (for example in control centres, medical expertise, technical expertise).
1.11	Insufficient information for training of operators and crew (vessel, ROC, terminal, drivers, …).
1.12	Inadequate procedures and liability maps.
1.13	Use of open fire on board or at the terminal (incl. Smoking).
1.14	Language problem between the involved stakeholders and workers
1.15	Lack of procedural understanding in cargo operation
1.16	Lack of common situational awareness of the operation
1.17	Poor planning quality or operational knowledge
1.18	The ability to stop loading or transport operations (access to control/operation system or contact with operational staff)
1.19	External service providers are not receiving authority to do maintenance work
1.20	External service providers are not familiar with the safety or operational instructions to perform their work
1.nn	…..l

3.1.2 Collaboration, low planning quality, information exchange between parties/ICT-systems, procedures

The subgroup collaboration covers sources of threats that are important when the dialogue between people/workers/drivers/providers and/or operators, where different organizations is to be handled, both internally and externally (e.g., between vessels, control centre and terminal workers). For example, it will be important for external service providers to be able to communicate with operators of an unmanned vessel. Collaboration is also important with regards to the handling of undesirable events (management and implementation), and thus which procedures are to be followed. In general, such procedures should clearly define who is responsible for various actions/incidents, the division of responsibilities between the actors involved in the transport system. Overall, therefore, the sources of threats are related to deficiencies, uncoordinated situational awareness, and inability to coordinate interaction between the actors involved.

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
2.1	Uncoordinated interaction between control centre, autonomous vessel, and with terminal services.
2.2	Loss of control centre capability to remotely assist autonomous operations (vessels, cranes, etc).
2.3	Inadequate and poorly rooted planning procedures for cargo handling
2.4	Limited opportunity to assist loading operations from a ROC, or from stakeholders involved in a loading process.
2.5	Language and cultural barriers between control centres and workers (non-English-speaking workers).
2.6	Different situational understanding between vessel and control centre.
2.7	Lack of collaboration possibilities between workers and operation centre, and with the stakeholders involved in the transport system.
2.8	Overloaded role for remaining staff in safety-critical operations.
2.9	Lack of interaction between crew, terminal workers, port authorities.
2.10	Lack of procedures for handling deviation/damage management (time, resources, equipment, damages, …)
2.11	Lack of documentation for cargo/load units to be transported (clearance, safety, insurance, etc)
2.nn	….

3.2 Technological sources of threats

The three subgroups that are placed under the threat source group technology category are:

(1) communication and technical,

(2) navigation, and

(3) vessels.

This group covers factors that are important for how the vessel should be able to sail safely, as well as how the vessel can be monitored, operated, and controlled from a control centre.

3.2.1 Communication and technical, remote operation, cyber attacks

The subgroup covers sources of threats that may arise due to problems with communication, loss of communication, but also proven actions that are intended to attack communication and technical solutions. Critical sensors should therefore be mapped, and possible back-up or redundant systems assessed. For example, errors in charging infrastructure have been included, which can mean that the vessel's energy supply is somewhat limited, which in turn can lead to a top event.

Table 6: Threat sources communication, remote operation, cyber attacks

#	Threats sources communication, remote operation, cyber attacks
3.1	Loss of communication between vessel/terminal/crane and control centre.
3.2	Errors on data and sensors (e.g., for fire detection, water intrusion, geofencing of cargo, temperature sensors, etc).
3.3	Lack of access to data for establishing situational awareness (for the ship's autonomy system and control centre).
3.4	Error on charging- and energy infrastructure.
3.5	Loss of communication for remote operation of equipment or vessel

#	Threats sources communication, remote operation, cyber attacks
3.6	Lack of knowledge regarding various on-board systems, terminal systems, operation systems and their capacities, and how they can be operated.
3.7	Lack of understanding of available land-based communication and technical infrastructure.
3.8	Loss of possibilities to communicate between involved ICT-systems (different management, owners, stakeholders, etc)
3.9	Error and downtime at the control centre.
3.10	Cyber-attacks or Computer attacks aimed at sensors and control system at the vessels, terminals, or control centres.
3.11	Loss of possibilities for situational awareness because of technical failures (CCTV, Communication, Navigation, Observation)
3.nn	…

3.2.2 Navigation and steering system and steering system, geotagging, geofencing

This subgroup is aimed at functional hazards that may arise during navigation and manoeuvring. Navigation-related threats are important to cover as they affect the vessel's ability to navigate and manoeuvre safely.

Table 7: Threats sources navigation and steering system, geotagging, geofencing

#	Threats sources navigation and steering system, geotagging, geofencing
4.1	Loss of navigation sensors or digital signals for navigation, steering or status
4.2	Machinery failure (i.e., reduced propulsion on a vessel).
4.3	Incomplete situational awareness (e.g., lack of understanding of traffic picture in operating area).
4.4	Lack of detection of objects in fairway (e.g., paddlers, leisure boats), or objects at a terminal.
4.5	Fault in / Insufficient dynamic positioning system on vessel, terminal, or crane
4.6	Loss of geotagging/cargo mark for loading or unloading operations
4.7	Non-compliance with ColReg.
4.8	Loss of possibilities of geofencing areas
4.9	Loss of sensors due to failures or low battery percentage
4.10	Loss of opportunities of remote operation
4.nn	…

3.2.3 Vessels, Crane, Port equipment and resources

Threats or damages on vessels, resources or infrastructure that can disrupt the performance.

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

#	Threats sources vessel, crane, port equipment and resources
5.1	Not detected water intrusion, leaks, and damage to the vessel
5.2	Control systems and equipment is damaged and cannot be used
5.3	Fire and / or smoke development in: engine room / battery room / lounge / control systems / cargo or other technological installations.
5.4	Failure in secure connection/interaction between vessel/resources and sensors in the infrastructure
5.5	Lack of standardisation such that vessel cannot use port infrastructure (i.e., energy loading point in infrastructure is not tailored to vessel position)
5.6	Lost opportunity for remote control of sensors, cranes, water doors and hatches.

#	Threats sources vessel, crane, port equipment and resources
5.7	Lack of detection of objects in fairways (e.g., fog and rain negatively affects sensors / camera).
5.8	Insufficient energy capacity on the vessel for loading activities, or for sailing.
5.9	Insufficient information sharing between systems and organisations
5.10	Loading system break down or failure
5.11	Crane Valve leakage
5.nn	…

3.3 External sources of threats

External sources of threats have two subgroups, 1) Threats sources Weather, Parts of the route is closed (sea-leg, terminal, gate, etc.), tide and low water, strike, etc. 2) Threats sources other external factors

3.3.1 Weather, Parts of the route is closed (sea-leg, terminal, gate, etc.), tide and low water, etc.

These are of both an operational and technical nature, and thus provide input as to which design requirements should be satisfied.

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

#	Threats sources Weather, Parts of the route is closed (sea-leg, terminal, gate, etc.), tide and low water, etc.
6.1	Operation is initiated at the wrong time (premature start of docking/crane operations vs. late start).
6.2	Lack of understanding of the time consumption regards operation.
6.3	Crushing injuries/damages when launching container operations, loading, and unloading containers from cargo deck at vessel or terminal.
6.4	Improper use of equipment.
6.5	Lack of information/instructions from the control centre, terminal workers, or crew regards operation.
6.6	Lack of understanding of (or overview of) the need to assist technology during a critical incident or operation (Operational Envelope)
6.7	Lack of coordination of an operation (e.g., between terminal workers and control centre, but also where external services/providers are involved).
6.8	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.
6.9	Wind or other MetHyd-forces makes it difficult to perform loading activities
6.10	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)
6.11	The terminal is not ready for the vessel
6.12	The vessel cannot be sailed in to port because bad weather
6.13	The vessel cannot be sailed in to port because of no pilotage available
6.14	The vessel cannot be served because of lack of terminal resources (workers, crane, terminal tractors, etc)
6.nn	…

3.3.2 Other external sources of threats

The group for other external factors summarizes sources of threats that are often outside the vessel's control, i.e., threats that are not controllable.

Table 10: Threats sources other external factors

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

4 Preventive and probability-reducing measures

The purpose of this section is to establish an overview of possible events and to suggest probability reducing measures. This will be done firstly by identifying possible threats that may have a triggering or amplifying effect against a possible top event. Such an overview is then used to identify potential barriers and measures of a preventive nature, and thus a probability-reducing effect against the identified top events. Figure 9 shows that a preventive barrier can be related to a specific threat source or have a function against several. This chapter summarizes some barriers and measures identified by the project in light of the AEGIS project's defined Use Cases, and thus not intended as a full coverage.

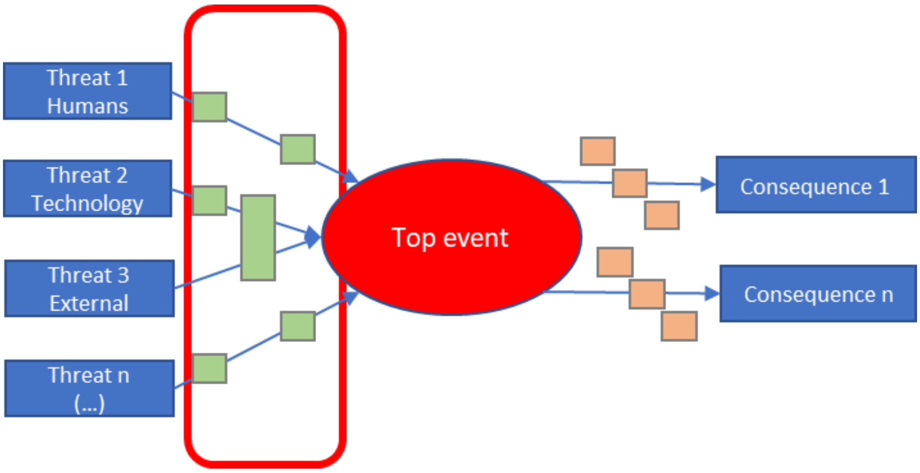

Figure 9: Preventive barriers for reduction of probability

4.1 Humans, organisational and operational

4.1.1 Preventive barriers and measures for threats associated with Terminal workers and crew, external service providers, terminal workers, operation centre

Table 11 Preventive barriers and measures for threats associated with Terminal workers and crew, external service providers, terminal workers, operation centre

#	Preventive barriers and measures for threats associated with Terminal workers and crew, external service providers, terminal workers, operation centre
1.1	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).
1.2	Install procedures for security personnel rejecting loads who pose a security threat.
1.3	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
1.4	Develop procedures/practices for allowing people access to the areas of operation
1.5	Develop systems for monitoring crew and guest on board
1.6	Develop secure infrastructure and solution for boarding (e.g., boarding at sea, boarding at terminal)
1.7	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
1.8	Develop intelligent and self-learning systems for object detection and situation understanding (sensor fusion) to avoid conflict between humans and technology.
1.9	Provide technical understandable information to involved humans, staff at the ROC and at the terminal (e.g., emergency posters and information screens).

#	Preventive barriers and measures for threats associated with Terminal workers and crew, external service providers, terminal workers, operation centre
1.10	Develop instructions/procedures for safety clearance of crew on board, terminal workers, and personnel at the control centre.
1.11	Implement easy access to security clearance of load units and cargo
1.12	Implement E-learning or other training programs for workers and operators
1.13	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)
1.14	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)
1.15	Implement digital twins/simulations to be used to train on an operation before executing
1.16	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.
1.17	Implement automatic sanity checks for manual data entries
1.nn	

4.1.2 Preventive barriers and measures for threats associated with Collaboration, low planning quality, information exchange between parties/ICT-systems, procedures

Table 12: Preventive barriers and measures for threats associated with Collaboration, low planning quality, information exchange between parties/ICT-systems, procedures

#	Preventive barriers and measures for threats associated with Collaboration, low planning quality, information exchange between parties/ICT-systems, procedures
2.1	Procedures for detection of unforeseen events in the transport system.
2.2	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).
2.3	Automatic counting of cargo units combined with lock system at quay facilities.
2.4	Guidelines and good communication with workers and external service providers, as well as with the ROC personnel.
2.5	Possibilities to contact involved via PA systems, information screens and emergency posters (multilingual).
2.6	Alarms with light/sound.
2.7	Design of a solution for communication between stakeholders (intuitive user interface).
2.8	Notification of ROC (Operation centres), responsibility and possibilities of remote operation
2.9	Allow humans to interact with technology and autonomous solutions
2.10	Integrated planning and shared information between involved in the transport system
2.11	Standardised information exchange when deviation, damage or not planned events happens
2.12	Guidelines on how humans can interact with autonomous technology
2.nn	…

4.2 Technological

4.2.1 Preventive barriers and measures for threats associated with Communication, remote operation, cyber attacks

Table 13: Preventive barriers and measures for threats associated with Communication, remote operation, cyber attacks

#	Preventive barriers and measures for threats associated with Communication, remote operation, cyber attacks
3.1	Implement redundancy in communication equipment for ensuring uninterrupted communication possibilities.
3.2	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.
3.3	Implement "Emergency Stop"-switch available to stop operations.
3.4	Implement fire walls or measures to avoid cyber attacks
3.5	Implement data security plan
3.6	Implement solutions for status monitoring of ships and systems, including technical condition measurement
3.7	Implement redundancy in sensors and other relevant solutions to avoid «single point of failure».
3.8	Implement plan for preventive maintenance of critical systems.
3.9	Develop procedures to transfer operational management between ROC's (in case of technical failure at a ROC etc.)
3.10	Develop procedures on "how to get back to normal operation" in case of technical failures happens
3.nn	…

4.2.2 Preventive barriers and measures for threats associated with the Navigation and steering system, geotagging, geofencing

Table 14: Preventive barriers and measures for threats associated with the Navigation and steering system, geotagging, geofencing

#	Preventive barriers and measures for threats associated with the Navigation and steering system, geotagging, geofencing
4.1	Implement redundant navigation solutions on critical technologies used for loading/unloading or transport.
4.2	Develop and implement MRC (minimum risk condition) barriers on critical technologies used in the transport system
4.3	Implement redundancy in critical sensors and steering systems to avoid «single point of failure»
4.4	Develop a contingency plan on possible failures on navigation and steering system, geotagging, or geofencing technology
4.5	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).
4.6	Implement geofence zones at the vessel for cargo operation, at the terminal, and for allowed navigation zones for autonomous technology.
4.7	Implement robust technology for object detection and situation understanding (also by sensor fusion).
4.8	Establish a CONOPS for the technology to avoid unwanted situations such as collision or conflict between humans and technology.
4.9	Implement possibility for decision support based on data from sensors in infrastructure

4.10	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)
4.11	Implement solutions for automatic tracking and tracing of cargo, load units, equipment, and humans
4.12	Implement Internal system health monitoring
4.nn	

4.2.3 Preventive barriers and measures for threats associated with Vessels, Crane, Port equipment and resources

Table 15: Preventive barriers and measures for threats associated with Vessels, Crane, Port equipment and resources

#	Preventive barriers and measures for threats associated with Vessels, Crane, Port equipment and resources
5.1	Implement remote monitoring of technical condition on transport means and cargo handling equipment
5.2	Install high-sensitivity sensors and alarms for early identification of fire and smoke
5.3	Install lights that informs others that it is an autonomous vessel, truck, or crane
5.4	Implement hatch for venting harmful fumes and gases in case of fire.
5.5	Establish plan for preventive maintenance of technology.
5.6	Develop contingency plan for new transport route if deviations in original plans occurs
5.7	Develop plan for use of new cargo handling technology/equipment/resources if origin fails
5.8	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
5.9	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

4.3 External

4.3.1 Preventive barriers and measures for threats associated with Weather, Parts of the route is closed (sea-leg, terminal, gate, etc.), tide and low water, strike, etc.

Table 16: Preventive barriers and measures for threats associated with Weather, Parts of the route is closed (sea-leg, terminal, gate, etc.), tide and low water, strike, etc.

#	Preventive barriers and measures for threats associated with Weather, Parts of the route is closed (sea-leg, terminal, gate, etc.), tide and low water, strike, etc.
6.1	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.
6.2	Implement a new route plan in case of weather or conjunctions do not allow original plan
6.3	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.)

6.4	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).
6.5	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.
6.6	Implement alarms on technical equipment, with light/sound and need for human interaction if required.
6.7	Develop learning materials such as a video that describes the autonomous technology in use, its limitations, and how to interact (humans vs technology)
6.8	Develop plan for different port quay visits as an alternative if weather predictions indicate conditions outside the operational envelope
6.9	Implement automatic shutdown when operational conditions are exceeded
6.n	…

4.3.2 Preventive barriers and measures for threats associated with Other external factors (e.g., other ship traffic, construction work)

Table 17: Preventive barriers and measures for threats associated with Other external factors (e.g., other ship traffic, construction work)

#	Preventive barriers and measures for threats associated with Other external factors (e.g., other ship traffic, construction work)
7.1	Develop CONOPS on how to operate the vessel/technology together with other traffic
7.2	Implement operational envelops where the time interaction between a ROC and technology is defined
7.3	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).
7.4	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
7.5	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.
7.6	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.
7.n	…

5 Reactive and impact-reducing measures

This chapter summarizes reactive barriers and measures identified by the project. The main purpose is to propose relevant barriers and measures that can reduce or eliminate undesirable consequences after a given top event has occurred. Like preventive and probability-reducing measures, the overview is not intended to be fully comprehensive, and case-specific assessments must be made.

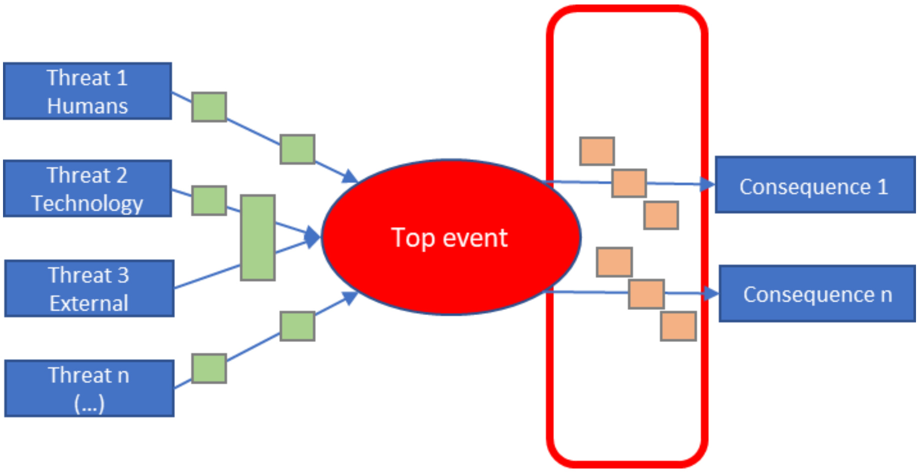

Figure 10: Reactive barriers for consequence reduction

5.1 Human, organizational and operational

5.1.1 Consequence reducing barriers for humans, organisation, and operational risk

Table 18: Reactive barriers: Terminal workers and crew, external service providers, terminal workers, operation centre

#	Reactive barriers: Terminal workers and crew, external service providers, terminal workers, operation centre
1.1	**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.
1.2	**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.
1.3	**Effectuate effective cargo handling:** Call for extra loading resources (workers, technology).
1.4	**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.
1.5	**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.
1.6	**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.
1.7	**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.
1.n	**…**

5.1.2 Consequence reduction barriers: Collaboration, low planning quality, information exchange between parties/ICT-systems, procedures

Table 19: Reactive barriers: Collaboration, low planning quality, information exchange between parties/ICT-systems, procedures

#	Reactive barriers: Collaboration, low planning quality, information exchange between parties/ICT-systems, procedures
2.1	**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.
2.2	**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.
2.3	**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.
2.4	**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.
2.5	***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.
2.6	**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.
2.n	…

5.2 Technological

5.2.1 Impact-reducing measures Communication, remote operation, cyber attacks

Table 20: Reactive barriers: Communication, remote operation, cyber attacks

#	Reactive barriers: Communication, remote operation, cyber attacks
3.1	**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.
3.2	**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.
3.3	**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?
3.4	**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.
3.5	**Initiate the use of other communication channels if main fails:** Start using back-up communication system if main solutions go down.
3.6	**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.
3.7	**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.
3.n	…

5.2.2 Impact reducing measures Navigation and steering system, geotagging, geofencing

Table 21: Reactive barriers: Navigation and steering system, geotagging, geofencing

#	Reactive barriers: Navigation and steering system, geotagging, geofencing
4.1	**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.
4.2	**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.
4.3	**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.
4.4	**Effectuate i*ncident navigation guidelines:*** Prepare guidelines for handling the autonomous equipment, e.g., vessel, in the event of a collision or grounding.
4.5	**Initialise Minimum Risk Condition:** In case of an uncontrollable event, either the technology or the ROC should launch the MRC procedures/safe state.
4.6	**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.
4.7	**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.
4.8	**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.
4.n	…

5.2.3 Impact reducing measures Vessels, Crane, Port equipment and resources

Table 22: Reactive barriers: Vessels, Crane, Port equipment and resources

#	Reactive barriers: Vessels, Crane, Port equipment and resources
5.1	**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.
5.2	**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.
5.3	**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.
5.4	**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. Similarly, it should be possible to use an autonomous vessel to tow external vessels in distress.

5.5	**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).
5.6	**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.
5.7	**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.
5.8	**Reallocate ship to different terminal:** In case the situation cannot be mitigated soon enough
5.9	**Reallocate ship to different port:** In case the situation cannot be mitigated soon enough
5.n	…

5.3 External

5.3.1 Impact reducing measures such as weather

Table 23: Reactive barriers: Weather, Parts of the route is closed (sea-leg, terminal, gate, etc.), tide and low water, strike, etc.

#	Reactive barriers: Weather, Parts of the route is closed (sea-leg, terminal, gate, etc.), tide and low water, strike, etc.
6.1	**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.
6.2	**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.
6.3	**Effectuate p*rocedures 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.
6.4	**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.
6.5	**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.
6.6	**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.
6.7	**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.
6.n	**…**

5.3.2 Impact reducing measures, other external factors

Table 24: Reactive barriers: Other external factors (e.g., other ship traffic, construction work)

#	Reactive barriers: Other external factors (e.g., other ship traffic, construction work)
7.1	**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.
7.2	**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.
7.3	**Effectuate new transport plan*:*** A new transport route/plan should be followed if planned route cannot be used for different reasons.
7.n	**…**

6 Example of using the framework

(note: the rest of this page is deliberately left blank)

6.1 Example of the bow-tie approach: Crane breakdown

In Figure 11 it is shown how the top event “#3.2 Crane Breakdown” is mapped to threats, preventive barriers, reactive barriers, and potential consequences. The numbering of the top event[3], threats, preventive and reactive barriers correspond to the tables shown in chapters 3-5 where the different components are described in more detail.

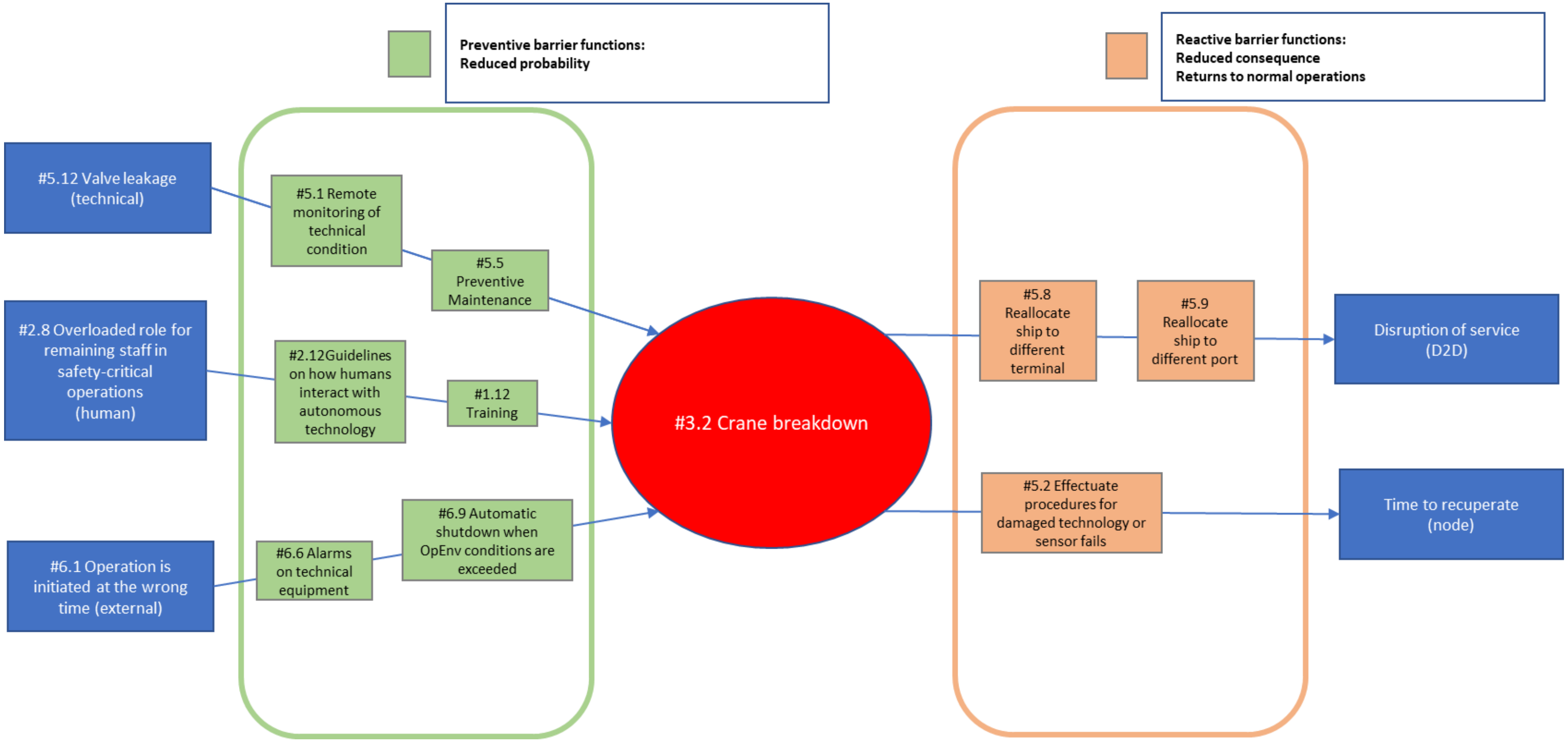
🟩 Preventive barrier functions:
Reduced probability
🟧 Reactive barrier functions:
Reduced consequence
Returns to normal operations
#5.12 Valve leakage (technical)
#2.8 Overloaded role for remaining staff in safety-critical operations (human)
#6.1 Operation is initiated at the wrong time (external)
#5.1 Remote monitoring of technical condition
#5.5 Preventive Maintenance
#2.12Guidelines on how humans interact with autonomous technology
#1.12 Training
#6.6 Alarms on technical equipment
#6.9 Automatic shutdown when OpEnv conditions are exceeded
#3.2 Crane breakdown
#5.8 Reallocate ship to different terminal
#5.9 Reallocate ship to different port
#5.2 Effectuate procedures for damaged technology or sensor fails
Disruption of service (D2D)
Time to recuperate (node)

Figure 11: Bow-tie diagram of a crane breakdown

[3] The top event is specified to “crane breakdown” as opposed to the more generic “Loading equipment not available”

6.2 Tabular example of the AEGIS methodology

Below we present application of the AEGIS methodology on basis of Step 1 where we decide to focus on the consequence of "Transport means not ready for loading". The steps below depict how to identify and pick relevant threats, preventive, and reactive barriers with the overall goal of getting the transport service back in operation.

6.2.1 Step 1: Identification of impact categories

Case: ***Disruption of service,*** **4.5 Transport means not ready for loading - late vessel arrival to port.**

As an impact category, this example focuses on disruption of services, at the same time as consequences related to late arrival vessels is elaborated. This referred to Table 1: Impact categories.

The impact could be as following:

1. The customer stops using the service
2. The reputation is decreasing
3. The cargo has to be rescheduled, cannot reach next transport means

6.2.2 Step 2: Choice of main hazards and top events

The top event in this example is shown in the next table. This referred to chapter 2.

Disruption of Service	Any disruption of the transport chain, resulting in unexpected delays or damage to or loss of cargo. Disruption could be a result from technical failures, operational or administrative issues, or could also be a result of external factors such as bad weather that leads to deviations.
Case:	Main carriage - 4.5 Transport means not ready for loading **(Late arrival vessel)**

6.2.3 Step 3: Selection of possible threats

Based on the current scenario, relevant threats are taken from the tables in Preventive and probability-reducing measures, it could also be own specified. In other words, the threats may have a triggering effect against, or in some other way may amplify, the actual top event.

Main identified threats

#	Main threats identified
1.14	Language problem between the involved stakeholders and workers
2.11	Lack of documentation for cargo/load units to be transported (clearance, safety, insurance, etc)
4.1	Loss of navigation sensors or digital signals for navigation, steering or status
6.12	The vessel cannot enter into port because of bad weather

6.2.4 Step 4: Identification of preventive barriers and measures

Next figure shows the link between the identified sources of threats and current barriers of a preventive nature. Note that the overview must not be regarded as complete, but more as an example of the application of the framework itself. The rows with green background shows possible threats while red colour background shows suggested barriers following the different threats identified.

#	Main threats identified and possible preventive barriers
1.14	**Language problem between the involved stakeholders and workers**
1.9	Provide technical understandable information to involved humans, staff at the ROC and at the terminal (e.g., emergency posters and information screens).
1.12	Implement E-learning or other training programs for workers and operators
2.11	**Lack of documentation for cargo/load units to be transported (clearance, safety, insurance, etc)**
2.3	Automatic counting of cargo units combined with lock system at quay facilities.
2.10	Integrated planning and shared information between involved in the transport system
2.11	Standardised information exchange when deviation, damage or not planned events happens
4.1	**Loss of navigation sensors or digital signals for navigation, steering or status**
4.1	Implement redundant navigation solutions on critical technologies used for loading/unloading or transport.
4.5	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).
4.9	Implement possibility for decision support based on data from sensors in infrastructure
6.12	**The vessel cannot be sailed into port because bad weather**
6.2	Implement a new route plan in case of weather or conjunctions do not allow original plan
6.3	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.)
6.5	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.
6.8	Develop plan for different port quay visits as an alternative if weather predictions indicate conditions outside the operational envelope

6.2.5 Step 5: Identification of reactive barriers and measures

In this step the top event has happened, and we should identify possible reactive barriers to limit the consequences of late vessel arrival. Following consequences have been identified

1. The customer stop using the service
2. The reputation is decreasing
3. The cargo has to be rescheduled, cannot reach next transport means

#	Main consequences identified and possible reactive barriers
1	**The customer stops using the service**
1.3	**Effectuate effective cargo handling:** Call for extra loading resources (workers, technology).
1.4	**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.
2	**The reputation is decreasing**
1.3	**Effectuate effective cargo handling:** Call for extra loading resources (workers, technology).
2.6	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.
3.6	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.
4.3	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.
3	**The cargo has to be rescheduled, cannot reach next transport means**
5.8	Reallocate ship to different terminal: In case the situation cannot be mitigated soon enough
5.9	Reallocate ship to different port: In case the situation cannot be mitigated soon enough
6.4	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.
6.6	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 Conclusions

In this report a methodology for assessing resilience of autonomous logistics chains has been presented, based on similar and conventional assessments within safety and security, the so-called bowtie. The methodology is presented with examples of the main elements such as threats, preventive barriers, unwanted events (top events), reactive barriers and potential consequences, all related to the execution of a generic autonomous transport chain. Then the focus was shifted to a specific resilience assessment of AEGIS use case A - Transport between the ports in the Trondheim region to Hitra Kysthavn, Sandstad, and further out to Rotterdam. The assessment was undertaken in collaboration with North Sea Container Line (NCL), the main industry partner and lead in the use case. The aim of the resilience assessment of use case A was twofold:

- To assess the foreseen AEGIS solution for the goods flow between the Trondheim area and Rotterdam
- To compare a current subset of the goods flow (utilizing trucks) between the Trondheim area and Rotterdam with the foreseen AEGIS solution for the same goods

In addition, the resilience assessment of use case A represents an initial validation of the proposed resilience assessment methodology developed in AEGIS. Special focus was given to ease of use, industry stakeholder involvement and completeness of the methodology.

The results from the resilience assessment of use case A can be interpreted, and taken into account on two different levels, the use case specific level and the overall autonomous shipping level. On a generic level, the resilience assessment show that autonomy introduces new threats (especially related to the interaction between humans and the autonomy and new maintenance models associated with unmanned operations), hereby increasing the need for new preventive barriers. In terms of unwanted events (top events), these seem to follow the same principles as conventional transport chains. The physical processes of loading/unloading, mooring/unmooring, and sailing, are still executed with the same overall purpose, albeit with a reduced human element. In terms of reactive barriers, mitigating the potential consequences of unwanted events, autonomy has an effect on certain conventional barriers involving human intervention, but autonomy also increases the room for action in terms of processes, procedures and operations which were not feasible with humans in the loop. For the consequences, one must separate between conventional reliability consequences such as delays and interruption of business and more safety related consequences. Removing humans from the loop, increases safety but in terms of pure resilience, the consequences follow the same pattern as conventional shipping. This, as the overall goal of shipping, moving goods from A to B, does not change when comparing conventional and autonomous shipping.

One of the key assumptions within autonomy is the enabling of a cost-efficient fleet of several smaller ships compared to the economy of scale of a fleet of fewer larger ships. In a logistic chain perspective, we see the positive effect of several smaller ships on two main elements in the risk assessment: a) an incident involving a ship, will have consequences for a smaller number of load units in the overall goods flow and b) the room for actions regarding mitigating measures (reactive barriers) increases, e.g., the number of back-up terminals which are suited to serve, and alternative routes, increases.

Regarding the comparison of the existing truck-based goods flow and the foreseen AEGIS-solution of for the same goods flow, a couple of characteristics regarding the truck alternative have been used as baseline: a) the tunnel from Hitra to the mainland, and b) The rush traffic in the Low Countries in general and in the Rotterdam area specifically. Issues such as statistical frequency of engine breakdown were disregarded as we do not have the required data to state the corresponding breakdown frequency for the AEGIS-solution.

References

[1] Onishchenko, O., Shumilova, K., Volyanskyy, S., Volyanskaya, Y., Volianskyi, Y (2022) “Ensuring Cyber Resilience of Ship Information Systems”. TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation, 16, Issue Number: 1, DOI: 10.12716/1001.16.01.04.

[2] Psaraftis, H.N. (2012) “Formal Safety Assessment: An Updated Review”. Journal of Marine Science and Technology, 17, 390–402.

[3] Stene T.M, Fjørtoft K.E (2020): Are Safe and Resilient Systems less Effective and Productive?”. e-proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference (ESREL2020 PSAM15).

[4] Weick, K.E. (1993) “The collapse of sensemaking in organizations – the Mann Gulch disaster”. Administrative Science Quarterly, 38(4), 628-652.

[5] Yang Wang, Enrico Zio, Xiaoyang Wei, Di Zhang, Bing Wu (2019) “A resilience perspective on water transport systems: The case of Eastern Star”. International Journal of Disaster Risk Reduction, 33, Pages 343-354, ISSN 2212-4209.

[6] AEGIS 859992 D7.2 Report on KPIs, DTU, February, 2021

[7] AEGIS 859992 D8.3 Bottlenecks and obstacles in Case A, Trondheim Havn, November 2022

[8] AEGIS 859992 D9.3 Bottlenecks and obstacles in Case B, DTU, November 2022