Resilience in autonomous shipping

K. E. Fjørtoft[1]

Ocean, SINTEF, Norway. E-mail: Kay.Fjortoft@sintef.no

O.E. Mørkrid[1]

Ocean, SINTEF, Norway. E-mail: Odd.Erik.Morkrid@sintef.no

In this article, we will look at some of the potentials within autonomous shipping and discuss how we can ensure resilience. The term resilience is widely used, Woods (2015) discusses four different common usages: (1) resilience as rebound from trauma and return to equilibrium; (2) resilience as a synonym for robustness; (3) resilience as the opposite of brittleness, i.e., as graceful extensibility when surprise challenges boundaries; (4) resilience as network architectures that can sustain the ability to adapt to future surprises as conditions evolve (sustained adaptability). Many factors affect the resilience approaches of the autonomous system, including communication and collaboration between technology and humans. This paper will give an understanding of technological limitations, as well as understanding of operational knowledge applied within shipping today that might be addressed to the autonomous sector. Will the knowledge at a Remote Control Centre be sufficient to recover from an unwanted situation? Will the autonomous system be capable to perform without human interactions? A bowtie methodology will be applied to identify and describe preventive and reactive barriers, which can be used to understand the resilience mechanisms. This paper will point to known operational challenges, focus on the interaction between technology and humans, and elaborate on issues which will be important drivers for increased resilience and a successful implementation of autonomous maritime transportation systems.

Keywords: Autonomy, Automation, Transport systems, Remote Control Centre, Safety, Resilience

1. Introduction

Maritime transport of goods and passengers is important to achieve sustainability and balance in the worldwide trade picture. If maritime transport stops, this will be critical for all of us. Maritime transport carries more than 90 % of global merchandise trade according to Mobility and Transport (2020). The accident with the *MV Ever Given*, the more than 20 000 TEU ship that grounded in the Suez Canal in March 2021, shows vulnerabilities in maritime trade that influenced the trade between Asia and Europe. The ship blocked the canal, and more than hundred ships were waiting for passage at both sides. About 12 % of global trade passes through the canal from Asia to Europe. As a result, many ships decided to sail the long way around the coast of Africa, which resulted in two weeks longer sailing time. We also experienced higher oil price because the supply to important markets stopped. The accident not only prevented the ships from sailing, but the pressure on the terminals at both sides was massive, as all ships entered the destination port at about the same time. This generated a space problem and demands to the terminal cargo handling equipment, as well as to the logistics out of the terminals. This accident shows the logistic vulnerability of the transport system as one incident can influence the transport picture worldwide.

Further discussions in this paper will be on implementing resilience in the autonomous shipping system where a set of vulnerabilities is described and where different autonomy levels are compared with levels of resilience. A bowtie methodology is used to identify barriers, with the purpose of understanding the resilience mechanism. One reason for this focus is that autonomous shipping is expected to grow and play a significant role in future maritime transport, and we should prepare for unwanted and unknown situations. The transport system must be trusted and be able to cope with potential crisis that may occur. There will be different stakeholders and systems involved in the operation of a Maritime Autonomous Surface Ship (MASS) as illustrated in Fig. 1. The Remote Control Centre (RCC) operators should control and plan the voyages, the software onboard the ship must be capable to identify traffic picture and own statuses and be capable to make its own decisions. We also have external stakeholders such as traffic centres, vessel traffic services, ports, terminal operators, governmental support centres and so on that takes part of the chain. All stakeholders have tasks and duties and the risk level is a summary of all risks related to technology and humans that are involved in an operation.

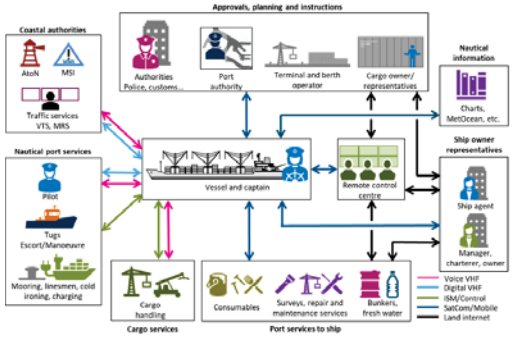

Fig. 1. Autonomous value chain. Source: SINTEF Ocean

Some risk elements in autonomous shipping can be technological, others are operational. Certain risk categories will be the same as for conventional shipping, and some will be new because of the introduction of autonomy and are yet unknown. We expect that automation will contribute positively and drive a reduction in total numbers of accidents compared to conventional shipping, Hoem (2019).

Proceedings of the 31st European Safety and Reliability Conference
Edited by Bruno Castanier, Marko Cepin, David Bigaud, and Christophe Berenguer
Published by Research Publishing, Singapore.
ISBN: 978-981-18-2016-8; doi:10.3850/978-981-18-2016-8_470-cd

2. Resilience

In a socio-technical system – including humans, technology and organisation – resilience is the ability to sustain required operations and achieve system goals under a large variety of conditions, including anticipated and unanticipated events, Schröder-Hinrichs et al (2016). 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 covers both vulnerability in design and external attacks. Vulnerability is a weakness, while an attack is an action performed by an attacker by purpose, Evensen (2020). There are several scientific projects and papers addressing resilience, as well as challenges related to safety and security for MASS. The EU project MUNIN (Maritime Unmanned Navigation through Intelligence in Networks), MUNIN (2016), was the first project to identify if and how it is possible for unmanned and large merchant ships to have the same, or even higher, levels of safety as conventional ships and highlighted both human and technological aspects. Tunggal says that when it comes to computers and computer networks we are talking about cyber-attacks as an important vulnerability. Attackers perform cyber-attacks to try to alter, destroy, expose, steal, disable, or gain unauthorized access to a network, infrastructure, computer system, or any other smart device, Tunggal (2020).

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). To address technological issues, it is important to build robustness and redundancy or to introduce options to recover from an unwanted situation. Hollnagel (2019) says that "A system is resilient if it can adjust its functioning prior to, during, or following events (changes, disturbances, and opportunities), and thereby sustain required operations under both expected and unexpected conditions." 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 MASS captain from sea to shore. 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 MASS automation system 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).

2.1. *Digitalization*

Digitalization is vital to improve the competitiveness of a value chain, and highly relevant when talking about automation and autonomous shipping (Mobility and transport 2020). As an example, from Mobility and transport, it is vital that maritime ports improve their position with respect to technological innovation and integration, both to ensure and improve their competitiveness, but also to reduce the cost for their respective users. This also requires that resilience must be planned for and barriers must be built. If something fails, there must be a recovery strategy. When increasing the digitalization of the maritime supply chain, this will also introduce new risks to the sector. Number of cyberattacks increased by 400 % in the maritime industry between February and May 2020, according to Captive International 2020[1]. In 2017, the shipping company Maersk and its international port operation wing overcame an aggressive cyberattack which served as a serious wake-up call. Other attacks have followed, and we know for sure that there will be more to come. Cyberattacks have become a main risk in the sector.

2.2. *The autonomous ship system*

The autonomous ships will have to interact with external sensors and systems. When staying in port, or sailing between ports, they will interact with both external and local infrastructure. For example, they will receive information from sensors in a port when docking. In the fairway, the sailing between ports, they must interact with other vessels, receive weather data from sensors and navigational aids from external sources, and interact with different stakeholders along their journey. The MASS must report real-time information to governmental bodies or to the RCC in command of the ships. The automation system will calculate its own capacities based on different factors such as internal (its own capacity, propulsion system, ballast and trim, technological condition, power consumption, etc.) and external factors (fairway conditions, weather, traffic, geography, digital infrastructure, etc.). Furthermore, it is also important to validate the communication link between the MASS and an RCC. Sometimes streaming of video is possible, other times the communication infrastructure will not allow transmission of high-capacity data at all. Technology awareness and the infrastructure capabilities must be counted for. One example of a new and valuable technology is a digital twin of the ship, where the RCC and operators can simulate operations before execution. Simulations can to a large extent reduce the likelihood of not being able to adequately cope with unknown events.

The autonomous ship system is a system of components that are dependent on digital communication to realize the overall functionality of an autonomous operation. The system will be more complex as there can be more than one RCC involved, e.g., to provide some degree of operational redundancy and, as indicated in Fig.

[1] https://www.captiveinternational.com/news/hackers-and-cyber-criminals-enjoy-increased-opportunities-in-2020-3798

2, both manual and automatic control can be distributed over several physical locations. In this paper we will not go into details on the actual configuration of a given MASS system but stick to a more general view. The distributed nature of a MASS also means that "situational awareness" for a MASS is a distributed phenomenon, where coordination between the components, hence digital communication, becomes a critical factor.

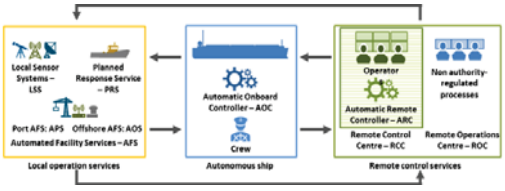

Fig. 2. Autonomous ship system. Source: SINTEF Ocean

2.3. *Situational awareness*

Situational awareness in autonomous shipping can be difficult to explain in a short context. It can be awareness to the operation, to navigational issues, to communication of data for navigational purposes, to ship condition, awareness to environmental issues, to the infrastructure, to regulations or to emergencies as examples. It can also be a combination of many of the mentioned elements. The degree of importance can differ, depending on the operational condition or to the MASS location. If the ship is about to dock there will be other types of awareness than when sailing in open waters, it might also be different when visiting a port in Norway compared to one in another country. Some important awareness types for a MASS operation can be:

Navigational awareness is to understand and describe the systems and the input used for navigational purposes. It is a complex picture where both on board systems as well as data from external sources are used as input to a decision made by either the RCC operator or the automation system on board a MASS. Several systems are needed to build an awareness, such as sensors for position, the traffic surrounding the ship, the metrological and hydrological conditions, and the ship's condition regarding manoeuvring capabilities. According to European Space Agency Industrial Policy Committee (2021) satellite navigation focuses on the mechanisms to determine the position of a given user and its course from one location to another, using satellites. Position, navigation and timing (PNT) is a combination of three constituent capabilities; ***Positioning***, is the ability to accurately and precisely determine locations and orientations two or three dimensionally. ***Navigation***, is the ability to determine current and desired position and apply corrections to course, orientation, and speed to attain a desired position. ***Timing***, is the ability to acquire and maintain accurate and precise time from a standard (i.e. UTC time zone) anywhere in the world and within user-defined timeliness parameters.

Communication is critical for autonomous systems and there are several types of communication systems or channels that can be used. Both terrestrial radio systems and satellite systems are relevant, the use depends on requirements to the data to be transmitted, as well as the geographical coverage. Also, agreements between operators and communication providers will be essential. In the context of communication systems, the quality of service (QoS) will be an important factor. QoS is the description or measurement of the overall performance of a service, particularly the performance seen by the users of the communication system, Fjørtoft (2021). To quantitatively measure QoS, several related aspects of the communication system are often considered, such as packet loss, bit rate, throughput, transmission delay, availability, jitter, security, latency, bandwidth, etc.

In the CySiMS[2] project, Cyber security in merchant shipping, new solutions are developed for authentication, encryption and securing integrity of information that is transmitted between ships, and between ships and shore. The idea is to implement solutions following the same approach as for bank identification, but where IMO, the International Maritime Organisation, will be the bank. The solution is a Public Key Infrastructure (PKI) where IMO acknowledges both sender and receiver of information, Rødseth (2020). It will be possible to implement this solution directly in the software or products, but it can also be possible to install a box in front of the systems. This is an example on a barrier that can be implemented to get a safer transmission of data.

Operational awareness is the understanding of whom you will exchange information with for an operational purpose. This means awareness to who will be responsible or in command of an operation, automation or humans, from where information for decision support can be received (sensors, systems, observations) or whom will be using the information (computers, systems on board a MASS, the navigators or the RCC). The awareness must reflect the real time picture as well as future prognoses of the picture, from seconds to hours.

Distributed awareness between an RCC and a MASS is to understand the operational and control picture between an RCC operator and the MASS automation system. Sometimes the MASS will have humans onboard, which requires that the RCC can exchange information with humans by voice, other times it will be necessary to interact directly with the automation systems at the MASS, Porathe (2018). Typically, the work tasks will be to solve operational challenges, such as navigation or maintenance orders at the MASS. A possible organisation of an RCC can be one operator controlling several ships, and where the operator has back-office knowledge from supervisors, engineers, or logistic personnel, example shown in Fig. 3.

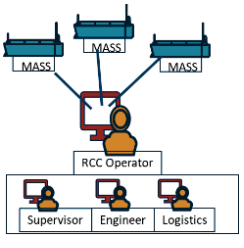

Fig. 3. Example RCC

[2] Cysims.no

We have proposed a framework for characterization of **distributed awareness** which is illustrated in Fig. 4. It shows the overall required situational awareness, divided into technical and operational awareness, which are depending on five underlying factors, where also some are dependent on specific operational specifications. A normal decision process is to retrieve data from sensors, do information acquisition, do situation assessment, analyse traffic prediction, to execute decision making, which result in an action in the end. From the left-most in the figure, the awareness will be to the communication facilities, where the QoS must be considered. Sensors and information from sensors will be used for information acquisition. Prediction of future development is for situation assessment, while definition of roles and responsibilities (human vs. automation) and decision making and control points to who is responsible for executing the decision. If something fails the MASS must enter a safe mode, or a minimum risk condition state, this if there are lack of information for decision purposes.

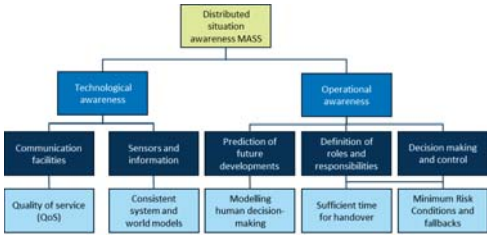

Fig. 4. Distributed MASS situational awareness framework. Source: SINTEF Ocean

A MASS system consists of physical equipment which is controlled by one or more automated controllers which in turn can be supervised and interacted with by humans at one or more locations. The control functions may, e.g., be organized on board the MASS or in an RCC with parallel connections to the equipment. There may also be a hierarchy of control functions where controls in the RCC connect to inputs to ship control systems. In the context of this paper, we are mainly interested in the effects of communication problems. Regardless of the actual topology, there are several vulnerabilities related to communication failures:

- An operator needs to have correct information about the relevant parts of equipment to issue the correct commands.
- Environmental sensors must be able to give operators appropriate information about environment factors for them to implement suitable/effective control strategies.
- A controller which controls two or more systems/units that have some form of interaction needs to gain updated information on the status to provide consistent instructions.
- Two controllers which control the same equipment, need to be synchronized or have well-defined responsibilities to avoid that conflicting instructions are sent.

The consequences of a communication problem will depend on the criticality of the control function. Relating to the input to the control function, one can generally define the following classes, Fjørtoft (2021):

i. A safety override/shutdown function, normally to a safe state. This means that the function may be conservative and shut down if, e.g., sensor or other input information is missing or obviously wrong. This may mean fewer direct safety problems, but too many shutdowns may cause a problem with the overall system availability.
ii. A safety related control functions with human supervision. This means that one in some cases can let the human do a sanity check of inputs and outputs, so that criticality of correct and timely incoming data becomes lower.
iii. A fully automatic safety related function or a function where the human has no possibility to assess sanity of inputs or outputs. This will be completely dependent on correct and timely input.

Thus, the highest safety concerns should be for the last category which also represents many of the control functions in an autonomous or highly automated ship. Still, the two other categories should not be disregarded.

3. Operational knowledge and challenges

3.1. *Humans and operational challenges*

Having a human in the loop also allows for a system design perspective that the automation system does not have to handle all possible situations the MASS can end up in. It will be possible to share the task responsibilities between the automation system and the human operator and let the human handle the tasks that technology struggles to handle. This obviously simplifies the design of the automation system and may in fact be what makes realisation of MASS more likely. However, it also means that the system design must include an interface between the human and the automation system. This interface must allow the human sufficient time to gain sufficient situational awareness to act correctly when needed.

3.2. *Interaction between automation and humans*

A critical factor when introducing a MASS is how the automation interacts with human operators with different roles. Important elements for modelling in this context are who will be owner of the different operations, either the RCC operator or the automation system on board a MASS. In some cases, we expect that the automation system is not capable to make the decisions itself and will therefore request the RCC operator to take control of the situation. This requires a hand-over process to be initiated, where time parameters are calculated to ensure that the hand-over process can be executed in time to build awareness and send new commands from the RCC to the automation system. If the operator/RCC is not able to take control, or there are failures in the communication link, this leads to a situation where the automation system will enter into a minimum risk condition state, awaiting assistance from the RCC operator.

3.3. *Technical indicators*

An operator at an RCC will be needing information from the MASS to take correct actions. It is important that the operator is not overloaded with information, while in some

cases it will be necessary to understand the sensor statuses/alarms and the reason for why an alarm is triggered.

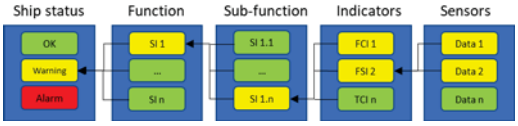

Fig. 5. Principles of status aggregation

Fig. 5 describes a sensor data hierarchy that in the end can lead to an overall ship status. In a status transmission from the ship to shore, only the top-level ship status node and any abnormal indicators with accompanying data sets, need to be transmitted. Too much detailed information could lead to an extra time constraint when a decision should be taken from an RCC. However, the message would in most cases also contain additional data values of interest, e.g., heading and distance to targets if the abnormality is related to collision avoidance as an example. This means that the RCC operator briefly gets an overall status and without delay assesses the origin of any abnormal ship status code. This will help to ensure rapid takeover from automation system by operator when problems occur. When a problem is detected, the operator can immediately start to investigate the most relevant technical systems to find the root cause of the problem. This avoids wasting time and bandwidth looking at irrelevant data.

4. Technological limitations

The following section describes some of the elements of concern regarding QoS and communication systems, where a brief reflection on the importance of MASS communication with an RCC is used as an illustrating case. In a general case, communication is used to connect distributed systems, where it is assumed that there are automatic control functions both in the RCC and on board the ship. In addition, there may be sensors and other support services on shore, e.g., automatic mooring. In all cases, the criticality of the communication link will be derived from the criticality of the functions that are dependent on the link. The operator will in many, but not all cases, be flexible enough to compensate for errors or low quality in the communication based on human intuition. Thus, communication requirements are mostly related to providing information to the operator in a timely and correct manner. Sometimes the automation system requests the operator to take control, typically because the automation system's operational capabilities are exceeded. These are critical situations in that the requested control transfer is necessary to avoid activating minimum risk conditions or fallbacks. Here, criticality will be linked to the time the human needs to gain situational awareness and be ready to safely take control. Correct and timely information is the critical parameter. However, the automation systems will often be faster than humans, hence requirements to QoS may be stricter. Jitter and latency can easily cause problems for automation. Bandwidth is dependent on application, but sufficient bandwidth is always a critical aspect, see the next section. Table 1 describes some bandwidth, latency and reliability requirements to operation types.

Table 1. Importance of QoS for three communication types

Type	Bandwidth	Latency/ Jitter	Reliability
Operator-Systems	M	M	M
Operator hand-over	H	L	H
Automation-system	H	H	H

L=Low, M=Medium, H=High

Thus, the safety of communication should normally focus on reliability and address latency, jitter and bandwidth as far as it is necessary for the intended task, Fjørtoft (2021).

4.1. *Cyber Security related to communication*

From a cyber security perspective failure modes of concern can be:

- Omission: Some information is lost by jamming
- Insertion: Some information is added to the data stream by spoofing
- Duplication: Old information is repeated, out of context
- Reordering: Information received out of sequence by duplication
- Modification: Information is changed (e.g., omission + insertion) by spoofing
- Impersonation: A message contains wrong sender or receiver information by duplication
- Timing: Too late (or possibly too early) information because of a DoS (Denial of Service) attack.
- Eavesdropping: Confidential information acquired by unauthorized party

The failure modes above can be addressed by introducing preventive barriers, some examples; 1) Digital signatures - integrity and/or authentication, 2) Sequence numbers and time stamps, 3) Encryption. The failure modes are independent of the causation factor being technical or arising from a hostile attack. Both have the same impact on the communication links and by that the overall safety of the system. The type of communication system, including transmission media and interface software in the connected nodes, will have an impact on how likely these problems are. This applies to technical problems as well as the possibility for hostile attacks. The five-step cybersecurity framework developed by National Institute of Standards and Technology (NIST) is one example for reducing cyber risks to critical infrastructure, Mobility and Transport (2020). This framework has been accepted as a tool to manage and reduce risks related to cyberthreats and focuses on five critical functions to increase cyber resilience: 1) Identify, 2) protect, 3) detect, 4) respond and 5) recover. Identify, protect and detect are all preventive barriers and respond and recover are reactive barriers to recover from a cyber security incident.

4.2. *Machine learning and artificial intelligence (AI)*

When introducing more automation and autonomy in the control systems for ships, there will also be more need for machine learning and artificial intelligence, especially for sensor fusion and situational awareness. For a fully autonomous ship with no human intervention there is a need for a highly complex autonomous system where

machine learning plays a key role. The ability to adapt to future surprises (ref. Woods' resilience definition 4) is the driver for a successful implementation of a fully autonomous ship and thus the quality of data used for training of the algorithms is paramount. The operational domain of the ship will be constrained by the data foundation used, Fjørtoft (2020). This link to data sets is one factor that makes an autonomous ship less suitable for changes in operational domain than conventional. The definitions of autonomy levels will follow Rødseth (2018) and explained later in this paper.

4.3. *Integration of and complexity of control systems*

The complexity of the control systems and the number of control systems being integrated on board, is increasing as technology evolves. The way of testing and verifying correct behaviour and failure resilience is lagging behind in this development. Traditional methods as FME(C)A (Failure Modes, Effects and Criticality Analysis) are no longer sufficient to ensure resilience with an increasing amount of software and integration of control systems, Rokseth (2018). The introduction of digital twins and simulator-based testing will help assessing this challenge and play an important role in building preventive barriers.

One potential preventive barrier could be a real-time simulation running 24/7 with input from the actual systems onboard the MASS and simulate the consequences of potential incidents. The results of these simulations could be presented with traffic lights (as in Fig. 5) and warn the operators at the RCC that there is a potential hazardous situation upcoming. One important challenge with this approach is the timing issue. In many cases, as goes for the sailing phase, time is extremely short for decision making.

4.4. *Different aspects of safety and security in autonomous ship systems*

The above discussions also point to several different perspectives on safety and security in distributed systems with mixed involvement of humans and automation, one of the characteristic factors of autonomous ship systems. This is not necessarily a complete picture and neither does it intend to give higher priority to certain perspectives. It is included to illustrate the complexity and the interactions between subsystems and components when assessing the overall safety and security of the system.

Functional safety is defined as "absence of unreasonable risk due to hazards caused by malfunctioning behaviour of electrical and/or electronic systems", Rødseth (2020). This is related to failure protection systems and, e.g., correct activation of fallback functions. This view may also have an impact on communication requirements. As an example, as functional safety is related to avoiding negative consequences once a hazard has emerged. Communication in this context may be more time critical. However, this will be dependent on the system design and the safety philosophy.

5. Assessing resilience using the bowtie methodology

The bowtie methodology in Fig. 6 could be used to assess the resilience and the four definitions herein. In the following, only three of the definitions will be used. Woods' third definition has intentionally been left out because it defines resilience as how the system behaves around the boundaries, both near and beyond, which is more related to operational performance than safety. Hence, the three definitions which will be used are: 1) Resilience being defined as rebound from trauma and return to equilibrium, 2) As a synonym for robustness and 3) The ability to adapt to future surprises (Woods's fourth definition, renumbered to 3 for convenience). These are included in the bowtie diagram. 1) Rebound from trauma is linked to the reactive barriers and 2) Robustness suggested to be linked to preventive barriers, where the idea is that a highly robust system should hinder (to a high extent) an unwanted event from taking place. 3) The ability to adapt is included together with an unknown, meaning that the system should be able to adapt to unforeseen threats, Hollnagel (2019).

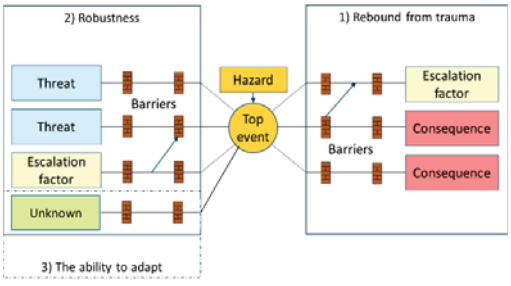

Fig. 6. Bowtie diagram linked to the definitions of resilience.

The left side of the bowtie in Fig. 7 is divided into operational (controllable), technological (controllable), and external (non-controllable) constraints. These are divided into awareness categories as described in chapter 3 (operational knowledge and challenges) and 4 (technological limitations) respectively, as shown in Fig. 4. The awareness categories are intentionally not one-to-one with the ones presented in Fig. 4, since sensors and information are replaced with cyber security in order to highlight the importance of the cyber security threats. The threats are included as examples based on discussions in this paper. The preventive barriers are kept on a high level and rather basic, such as 2-factor authentication as a cyber security barrier and redundancy as a communication barrier. Technological and operational reactive barriers, as well as external barriers such as rescue services, are included as examples, as well as two examples on consequences if all barriers fail. The whole picture defines the resilience, and one could argue that the system is not robust enough if one cannot avoid the consequences, either through preventive or reactive barriers, hence the resilience level is not sufficiently high. A high level of resilience would be linked to identifying the awareness areas and corresponding threats, implementing solid protection and detection measures, and establishing response and recovery measures to make sure the MASS fulfils the four resilience definitions to a high extent. Further discussion related to level of resilience takes place in section 5.1.

5.1. Reading resilience from the bowtie assessment

Going back to Woods' resilience definitions: The ability to adapt, resilience as a synonym for robustness and the ability to rebound from the top event (trauma), will define

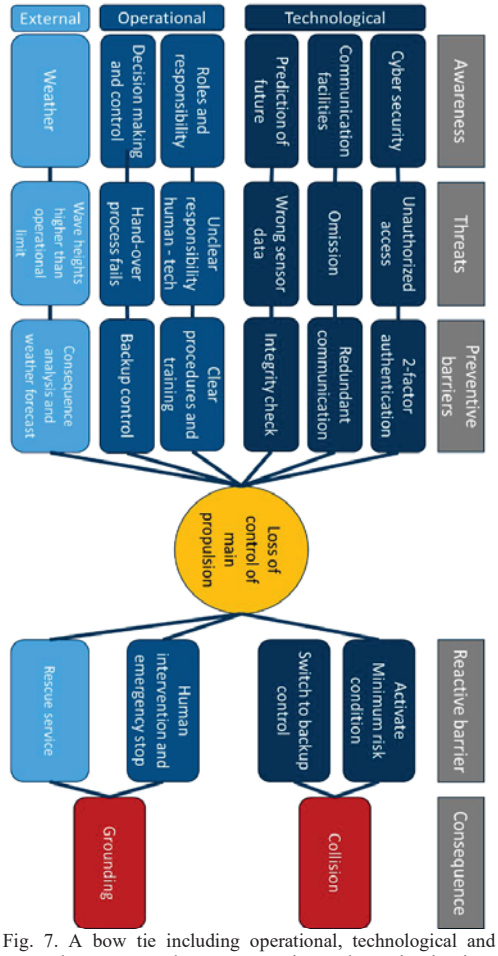

Fig. 7. A bow tie including operational, technological and external awareness, threats, preventive and reactive barriers. Source SINTEF Ocean

the level of resilience. If the MASS successfully returns to equilibrium, being the normal situation before the trauma, is the resilience then defined as being at the highest level? And how did the MASS return, by human intervention or solely by technological means? It is hard to talk about resilience for a MASS perspective without tying it to human interactions. If the MASS could not return to equilibrium without human intervention, is the MASS then not robust enough and hence the resilience is at a lower level? There is a need to define levels of resilience, in the same way as we define levels of autonomy. And these levels will have to depend on the level of human operation or intervention. AL0-1 (decisions support, operator controlled) and AL2 (automatic) exist today as e.g., auto pilot and dynamic positioning, both with crew assisting on board. AL3 (partly and constrained autonomous) will be the most probable autonomy level in near future, according to Rødseth (2018). In AL3 the automation system can perform certain tasks, constrained by limits to the actions it can take without human approval. AL4 (constrained autonomous) is defined as autonomous operation, but with constraints like limits to speed and track deviations. AL5 is defined as a fully autonomous operation with no operational constraints or operator involvement. Fig. 8 shows the correlation between three proposed levels of resilience (LR1-3) and the five levels of autonomy, and how these are assessed with respect to humans and technology. A basic level of resilience (LR1) equals today's level of resilience for a conventional ship at autonomy level 1 or 2. In order to achieve a high level of resilience for AL3-4, the intermediate level of resilience (LR2) is needed, as these autonomy levels introduce increased automation and decreased human operation and will affect resilience as we need to build more technological barriers and assist the humans even more. The highest level of autonomy requires an advanced level of resilience (LR3), which is regarded as a theoretical max level where the MASS is fully autonomous and has all possible preventive and reactive barriers implemented.

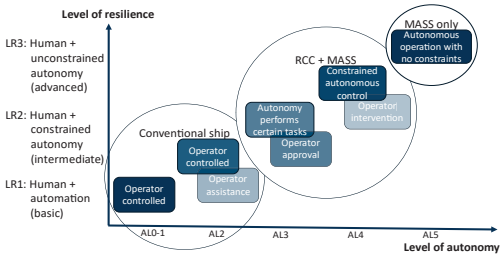

Fig. 8. Levels of resilience w.r.t level of autonomy. Source SINTEF Ocean

The three levels of resilience are described as follows:

- *LR1, Basic (AL0-1-AL2):* This resilience level includes barriers that are relevant for conventional ships where humans are in control and assisted by automation, such as extra crew on board and redundancy of critical components.
- *LR2, Intermediate (AL3-AL4):* Different barriers compared to LR1, as the crew is moved to an RCC. More focus on hand-over between automation and RCC operator and technological barriers that are feasible due to more autonomy and automation on board. Resilience-focus moves from an operational to a technological perspective, where humans are the back-up solution. Redundancy in communication is critical. Operator knowledge at the RCC must cover what today is critical crew on board (such as electricians, machinists etc.)
- *LR3, Advanced (AL5):* At this level, all preventive barriers are technological and there are no operators in the loop, unless an incident happens. Hence focus on barriers must be technological and the requirements to testing and verification of software reaches a higher level. Barriers related to traffic control centres, RCCs and other ships are crucial. Redundancy requirements will probably reach a new level. Most reactive barriers at this level will probably have to be external and linked to human intervention.

The question is: Can a MASS become more resilient than conventional ships? If so, it must be proved that LR2/3 > LR1. The bowtie methodology can be applied to show

that it is likely that LR2/3 > LR1. LR3 is at a very different level than LR1/2 because this is currently just a theoretical level. Risk (probability and consequences) needs to be assessed in order to answer the above question. This paper will not cover this analysis, as it is regarded as a supplement to the bowtie, which is the key focus here.

Sustained adaptability is another topic which from the authors' understanding, is defined as the ability to adapt to unforeseen events and sustain this adaption, meaning that the next similar event will not be an unknown, but rather a known event which the system could react to without human intervention. Eventually, a MASS will become more resilient given that the AI is based on high-quality data from the correct operational domain.

Conclusions

From our study we have seen that:

- Resilient systems are important when designing autonomous transport systems. It should be planned for both technological and operational contexts. The challenge for both is to handle normal variations, surprises and changes in operational performance.
- Situational awareness in autonomous systems is also important. The awareness must be tailored to the users of the observation, either the automation systems or the humans. Resilience is a suitable approach when studying technological innovations (autonomy). A preventive approach, in addition to a traditional, is necessary to cope with foreseen/unforeseen events.
- A bowtie diagram is a well-suited method to be used when identifying preventive and reactive barriers.
- There are synergies between Woods' resilience definitions and the bowtie methodology as ability to rebound from trauma, robustness, and the ability to adapt to surprises are all important factors when designing barriers, both preventive and reactive.
- The levels of resilience as well as types of barriers that can be used within autonomous operations will be different depending on the level of autonomy. There will be a gradual decrease/increase in technological and operational barriers depending on the autonomy level. As an example, AL5 will have to include more technological barriers than AL0-1 or AL2.

Some important elements that future studies of autonomous shipping should consider:

- Resilience barriers should cover both unexpected and expected changes. The barriers must be built to adapt to unexpected changes.
- Preventive and reactive indicators are needed, and they should be context specific.
- Planning at, and coordination between, different levels and actors are essential. Think integrated transport systems instead of modal focus.
- Explore the total effects of introducing MASS when it comes to resilience skills and develop specific training of different actors and levels.
- Coupling of resilience definitions and risk probability in order to build efficient and robust barriers.
- Looking closer into Woods' third resilience definition on operational performance around system boundaries

Acknowledgements

This work has been partially funded by the Norwegian Research Council projects IMAT and SAREPTA. It has also received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 859992 (AEGIS).

References

Accelerating digitalization (2020) – Critical actions to strengthen the resilience of the maritime supply chain. Mobility and transport connectivity series.

Evensen Marte Hvarnes (2020). Master Thesis: Safety and security of autonomous vessels

EUROPEAN SPACE AGENCY INDUSTRIAL POLICY COMMITTEE, Information Note, Discovery, Preparation, Technology Development, Preliminary Selection of Activities for the TDE Work Plan, 2021-2022

Fjørtoft, Rødseth, ESREL (2020): Using the operational envelope to make autonomous ships safer

Fjørtoft, Rødseth, (2021). H8 Situational awareness in autonomous maritime operations. The project Sacomas.

Hoem (2019): TransNAV 2019: Addressing the Accidental Risks of Maritime Transportation: Could Autonomous Shipping Technology Improve the Statistics? [Å.S. Hoem, K Fjørtoft, ØJ Rødseth], ISSN 2083-6473, e-ISSN 2083-6481

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

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

Porathe T., Hoem Å., Rødseth Ø.J., Fjørtoft K., Johnsen S.O. (2018), At least as safe as manned shipping? Autonomous shipping, safety and "human error".

Rødseth Ø.J., Faivre J., Hjørungnes S.R., Andersen P., Bolbot V., Pauwelyn A.S., Wennersberg L.A.L. "AUTOSHIP deliverable (2020) D3.1: Autonomous ship design standards", Revision 1.0. Retrieved from https://www.autoship-project.eu/downloads/ (2020).

Rødseth Ø.J., Nordahl H, Hoem Å (2018). Characterization of autonomy in merchant ships

Rødseth Ø.J. et al (2020) The need for a public key infrastructure for automated and autonomous ships. IOP Conference series: Materials science and engineering. ISSN 1757-8981.

Rokseth B, Bouwer, Utne I., Vinnem J.E. (2018) Deriving Verification Objectives and Scenarios for Maritime Systems Using the Systems-Theoretic Process Analysis

Schröder-Hinrichs Praetorius, G., Graziano, A., Kataria, A. and Baldauf, M. (2016). Introducing the Concept of Resilience into Maritime Safety. In: P. Ferreira, J. van der Vorm, D. Woods (ed.), Proceedings: 6th Symposium on Resilience Engineering: Managing resilience, learning to be adaptable and proactive in an unpredictable world. 22nd-25th June 2015 at Lisbon, Portugal (pp. 176-182). Sophia Antipolis

Stene T.M, Fjørtoft K.E (2020): ESREL 2020: Are Safe and Resilient Systems less Effective and Productive?

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

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

Woods, D.D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. Reliability Engineering and System Safety 141, 5-9.