Using the operational envelope to make autonomous ships safer

K. E. Fjørtoft[1]

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

Ø. J. Rødseth[1]

Ocean, SINTEF, Norway. E-mail: OrnulfJan.Rodseth@sintef.no

The introduction of autonomous shipping as a new transport form is about to start. Defining exactly what situations the autonomous ship must be able to handle, here called the "*operational envelope*" is obviously important. This will be the basis for assigning responsibilities to humans or automation, for designing the human-automation interface and for testing and approval of the automation systems. There are various ways to define the operational envelope and the associated automation or human executed tasks. The importance is to refer to the awareness of a situation and to give the perception of an event with respect to time and condition, and the system behavior, actual and future. It will address the human factors by detail plans for a situation and automation awareness. It will give an understanding between automation and human role, give user experiences and usability of the solutions. An operational envelope main purpose is to describing the characteristics of a proposed system. It is used to communicate the quantitative and qualitative system characteristics to all stakeholders. This paper will examine the general requirements to the operational envelope and the description of the associated tasks and will look at some methods that can be used. It will be built on experiences from the different transport modes, as well as from the literature.

Keywords: Autonomy, automation, transport systems, remote control centre, safety, resilience, maritime

1 Introduction

Industrial autonomous vehicles are robots with a high degree of automation, high cost, high damage potential and which need to operate economically in a commercial environment (Grøtli et al., 2015). This requires a development process, including the early concept design, that is geared towards minimizing costs while ensuring safety and operational effectiveness. This in turn means that virtually all industrial autonomous vehicles will have some degree of human supervision and control due to their high value and general safety constraints. Having a human in the loop also allows a design where the automation does not have to handle all possible situations the vehicle 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 automation have problems to tackle. This obviously simplifies the design of the automation system and may in fact be what makes autonomous ships more likely than autonomous cars, at least in mixed traffic. 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 enough time to gain sufficient situational awareness to do the correct actions at the right time. This paper will introduce the "operational envelope" as a tool to describe the cooperation between the human operators, either onboard the vessel or at a remote operation centre, with the automation system. The operational envelope is based on the concept of the "Operational Design Domain" that was introduced in SAE J3016 (2016) and was developed further for use on autonomous ships in Rødseth (2018). The name was proposed changed to operational envelope during the work on the ISO 23860 terminology standard (2019) for marine autonomous surface ships (MASS). At the time of writing, the terminology work is still ongoing, but the paper will use the term "operational envelope" in the following text.

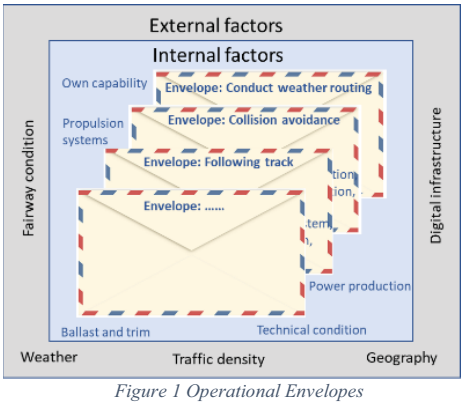

Figure 1 Operational Envelopes

As illustrated in Figure 1 there can be several envelopes that together play a role in an operation. Within each of them both internal and external factors will influence the performance, or the interaction needs between the automation and the operators.

Proceedings of the 30th European Safety and Reliability Conference and
the 15th Probabilistic Safety Assessment and Management Conference
Edited by Piero Baraldi, Francesco Di Maio and Enrico Zio
Published by Research Publishing, Singapore.
ISBN/DOI: TBA

This paper will give an overview of the operational envelope (OE) and its place in the development process for industrial autonomous vehicles. This includes the concept of Ship Control Tasks (SCT) which are the technical and procedural realization of the control functions needed to realize the OE. The paper will then go through some of the proposed uses of the OE and SCT for analysis of system characteristics, including human factor issues and safety.

2 Autonomy and human-automation interface

A commonly referenced and early definition of levels of *automated decision making* was proposed by Sheridan and Verplank (1978). This defines 10 levels of gradual transfer of control from human to computer, e.g. from the computer just proposing a set of possible actions, via the computer recommending one particular action to various forms of direct action by the computer. A similar scale, but reduced to five levels, was proposed by Endsley (1987).

An extended principle was proposed by Parasuraman et al. (2000). Here the decision process is divided into four steps: 1) Data acquisition and sensory processing; 2) Information analysis or perception; 3) Decide action; and 4) Execute action. The level of autonomy or automation can then be applied independently to these four stages. This could be called a form of *decision pipeline autonomy*. A variant of the pipeline principle has been proposed by Endsley and Kaber in (1999). This has reduced the full matrix from the previous authors into ten discrete levels that capture the most relevant combinations. SARUMS (European Defence Agency's Safety and Regulations for European Unmanned Maritime Systems) has defined six levels of control which are similar to the pipeline principle. This is also referenced by the UK MASS Conduct Principles and Code of Practice (2019).

Another approach has been taken in the definition of levels of automated driving (SAE 2016). This is very similar to the definition The Rhine Commission uses for inland waterways automated navigation (CCNR 2018). Both scales have six levels which is capturing both a higher degree of abstraction of the control task, from just steering assistance to control of several vehicle processes, as well as lower involvement of the human, from direct command via monitoring to a fallback role. The CCNR definition also opens up for remote monitoring or control, which is not normally applicable to cars. This principle could be called *hierarchical control autonomy*.

Note that Inagaki and Sheridan (2019) raised a critique against the SAE "conditional automation" level. They argued that there should be an additional level where it is explicit that the automation will take the system to an minimum risk condition if the user fails to respond in time, alternatively that conditional automation explicitly was redefined to include this requirement.

There are numerous other principles for definition of automation or autonomy levels. One final example is ALFUS (Autonomy Levels For Unmanned Systems) that uses a capability matrix definition, based on mission complexity, environmental difficulty and human independence (Huang et al. 2005).

All the above definitions address the division of responsibility between human and automation, with different emphasis on what is important in the interaction (complexity, hierarchical decision making, pipeline approach etc.). In this paper we only focus on one factor: When the operator is required to take control, how long does he or she have to make the best decision about what to do next?

3 The operational envelope and the ship control tasks

The results published in this and the next section are based on previous work published in Rødseth (2018), and from analysis of the logistical planning processes within the energy sector (Ose 2013). Some more details of the operational design domain (ODD, now called the operational envelope) can be found there. Nomenclature and terminology have been updated to reflect new proposals from the terminology standardization work.

The operational envelope for the autonomous ship system provides the definition of what conditions the ship can operate under. Thus, the OE can be looked as a form of a multi-dimensional state space where each tuple (s, e) of a specific state vector *s* and an event *e* that can occur in this state, should be included. This also includes events related to "anticipated failures", i.e. technical problems that the system is designed to handle during normal operation. In some cases, one may want to look at the OE as time-varying, as not all tuples are relevant in all voyage phases. The operational envelope will be called $\boldsymbol{O}$ in the following.

$$\forall\ (i,j):\ (s_i,e_j)\ \in \boldsymbol{O} \qquad \text{Eq. 1}$$

The operational domain may have to be subdivided into separate sub-domains to reflect voyage phases (L: Leaving berth, D: Departing port; C: Coastal etc.) and different functions (V: Voyage planning; S: Sailing; O:Observation; F:Fire etc.). This is illustrated in the Figure 2 where function is subscript and phase superscript. The actual structure will depend on the case at hand.

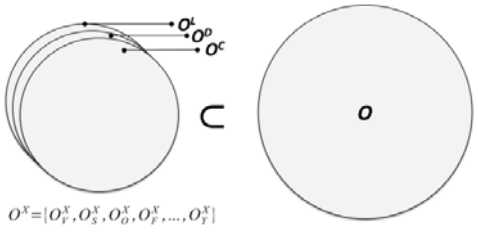

Figure 2: Operational Envelopes by function and phase

During the design process, $\boldsymbol{O}$ may also be split into different regions by who has the responsibility for performance of the control task related to each state and event pair. This is illustrated in Figure 3.

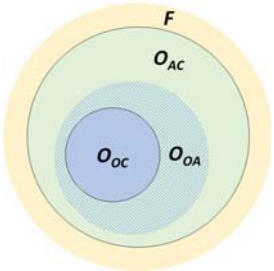

Figure 3: Operational envelope by task responsibility

The regions shown here are:

O_{AC}: States and events that the automation system is designed to handle alone, with human interaction being not necessary.

O_{OC}: States and events that must be supervised or executed by the human operator. The automation system is not designed to handle these by itself. In this paper human operators can be located either on board the vessel, or at a remote control centre, the RCC.

O_{OA}: States and events that the automation system may be able to handle, but where human intervention is required if the automation system fails to find a safe and effective solution. This can typically be the case when artificial intelligence type systems are used, and where it is not known if all the specific cases will have a viable solution.

F: Fallback states, also called minimum risk conditions (MRC), that are used in cases where events will take the system out of planned for states and event, i.e. out of O. This may happen due to unanticipated failures, environmental conditions outside O or failure of an operator to respond when the system requires human intervention.

For each of these regions, the designer needs to assign a task to each relevant (s, e) pair that can safely and effectively handle the situations and, if necessary, move to a new operational envelope state. These tasks are called the Ship Control Tasks (SCT) and will correspond to the same regions as O.

4 The importance of detail planning

There are different levels of planning regards time and detailing; Strategic, Tactical and Operational planning is used in many sectors, Ose (2013). There are different requirements to the planning precision and time period regards the different stages. In this paper we have used following definitions; Strategic planning is the 1 – 5 years perspective. Tactical is a perspective from 14 days up till 1 year. Operational is normally more detailed and precise where the time is between today and until 14 days in front.

All these levels have different focuses and constraints which need to be handled, but they should have a strong link to assure that the plans are sufficiently connected. This means as an example that tactical planning identifies critical resources to be allocated the vessel, while the operational planning is planning what time they should be used according to the voyage plan with schedules that are coordinated with work tasks and other activities for the vessel.

In the context of planning there are different constraints to be aware of in the different planning phases. Some of them is possible to control, while others are uncontrollable which means they are forces outside control that influences the outcome of the plan. For the purpose of this paper the operational planning will be elaborated, where the voyage plan is important input for successful sailing. The operational plan will for instance include the envelope "following track", that will define the waypoints for the vessel, where to provide status reports, where to be remote operated, where people should be placed into the loop and so on. The next table summarises some of the constraints that should be considered in the different planning phases.

Table 1. Different constraints on the different planning levels.

	Controllable constraints	Uncontrollable constraints
Strategic level	Prioritization between operations, Strategic partnership, Information technology, Life cycle management, Resource needs (people, knowledge, equipment, facilities, vessel, logistics demand)	Market and financial issues, Infrastructure and Governmental decisions (distribution centers), Laws and enforcement
Tactical level	Critical resource (People, Equipment, Vessels), Transport demand (vessels, storage, on-board, base), Sourcing contracts, Routing and scheduling of fleet, Organization between RCC and MASS, Inventory decisions, Transportation strategy, Demand knowledge, Risk and safety evaluation (HSE), Maintenance planning	Financial issues, Market changes/fluctuations, Technology failure, Infrastructure and Governmental decisions (distribution centers), Laws and enforcement
Operational level	Resource management, Stowage, Daily production and distribution plans, Status reports and scheduling, Inbound/Production/Outbound operations, Risk and safety evaluation (HSE), MASS control and hand-over plans between AC and RCC.	Weather, Strikes, Damages, Traffic, Deviations, 3rd part failures, Changes in demand

The Convention on the International Regulations for Preventing Collisions at Sea, COLREG, is a regulation defining the rules at sea to avoid collision between vessels (IMO COLREG). The COLREG will be important for autonomous shipping. But there are some unclear factors to be elaborated in to the regulation, for example the role of a RCC when a vessel is sailing without crew on board, as well as requirements to hand-over processes from automation to operators, either located on board the vessel or at a control centre.

5 Automation or autonomy

In general, it is very difficult to find a technical definition of autonomy and automation that can clearly differentiate between the two. This has led, e.g. the Society of Automotive Engineers to suggest that the term autonomous is avoided and that automation or driving automation is used instead (SAE 2016). In the work on the new ISO 23860 standard (2019), the following definition have been proposed:

Automatic: *Pertaining to a process or device that, under specified conditions, can function without human intervention (this definition is based on ISO/TR 11065).*

Autonomous: *In the context of ships, autonomy e.g. as in "Autonomous Ship", means that the ship use automation to operate without human intervention, related to one or more ship processes, for the full duration or in limited periods of the ship's operations or voyage.*

The differentiation here is that automation is the same concept in both cases, but to be autonomous, the computer can take decisions without a human to oversee or control it, DNV GL (2018)

Another issue will be to understand the hand-over between autonomous execution or control, to direct remote control or indirect remote control. Figure 4 describes such a scenario, that also indicates how to hand-over control from automation to humans, and vice versa.

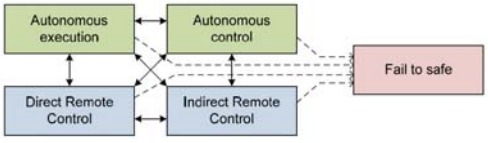

Figure 4 Main ship modes

The full set of five modes is defined as follows:

- Autonomous execution: The ship follows a predefined "program" supplied by the operator or RCC. Does not need intervention from operator/RCC, except for periodic updates of plans etc.
- Autonomous control: The ship deviates from predefined plans within operational envelope allowed for by operator or RCC. Does not need intervention, except for periodic updates of plans etc. The parameters is defined in the envelope.
- Indirect Remote Control: Ship is under control from operator or RCC giving instant "plan updates" to the AC (Autonomous Ship Controller). The AC is transferring these to new set- points and controls to ship systems. AC does not otherwise interfere with operator or RCC instructions.
- Direct remote control: The operator or RCC has taken over all direct control of ship systems. AC is not participating or interfering in control operations.
- Fail to safe: This should be more correctly called a Minimum Risk Condition (MRC) as safety cannot always be guaranteed in this mode. This mode can be entered, e.g. if the ship has lost contact with the operator or RCC and has identified a condition, where an update from them is needed or after some other unanticipated failure.

In this case, the automation system must select one of several predefined MRC procedures. The MRCs are not considered part of ***O***. This could be to let the ship be waiting for the operator or RCC, or eventually an emergency control team to re-establish contact with the ship. MRC may also be invoked if the operator is slow in responding to a critical situation when his or her attention is needed.

An unmanned ship will in most cases use a remote-control centre to provide high-level monitoring and to ask for assistance when the automation reaches its limits. Considering the above definitions, this means that the operator needs to change from either monitoring the ship, or even doing completely other tasks, to first achieve situational awareness and then do the necessary actions and establish control. This will take some time. In this paper, the time interval from when the automation warns about the need for human assistance to the human operator is able to give the correct response, will be called the maximum response time or T_{MR}. This will depend on the operational procedures on the ship and the RCC and from what state the operator starts when his or her actions are required.

The other important time interval is the response deadline or T_{DL}. This is the worst case, i.e. potentially shortest time from a potential problem is detected by the automation to the automation has to activate a fall-back procedure and enter an MRC.

The maximum response time can also apply to the crew on board. A relevant application of autonomy on manned ships is to control the ship, when the ship crew is sleeping or doing other tasks on board the vessel. This has the same constraints in timing: The crew must get back to their control position and then get an overview of the situation to safely regain control. However, the response times for RCC crew and sleeping crew on board is quite different.

Many publications have suggested different ways to define "levels of autonomy". See Rødseth (2018) for a discussion of this issue for ships and references to some relevant definitions. Most definitions of "levels of autonomy" has a specific application area in mind and the above differentiation in times to regain control (T_{MR}) can also be used to define "levels of autonomy". In the following, a number of such levels are defined. The time parameters used in the examples are only meant as indicative and may change as more research on this issue has been performed, they are based on experiences from conventional shipping:

1. *Operator in control:* The operator is directly in control of the ship. Hand-over time is not relevant ($T_{MR} = 0$).
2. *Operator supervision:* Automation is used to assist operator, and operator is overseeing the operation and needs only a short time to gain situational awareness when actions are needed (e.g. $T_{MR} < 10$ s).
3. *Operator at site*: An operator is at the control position but is working with other tasks and will need time to gain situational awareness. This could be on the order of a minute or so (e.g. $T_{MR} <$ 120 s).
4. *RCC operator:* A remote operator in the RCC is needed to resolve the situation. This could be similar to the previous (e.g. $T_{MR} < 120$ s) if the RCC operator needs to be mobilised from other tasks.
5. *Operator available:* The operator is available, but is in another location, possibly sleeping, and will need several minutes to reach the control position and to regain safe control (e.g. $T_{MR} < 10$ min).
6. *No operator:* There is no operator and automation must be able to handle all operations by itself

(T_{MR} is the duration of the operation or the voyage).

6 Interaction between automation and humans

A critical factor in the use of autonomous ships in mixed traffic is how the automation interacts with human operators in different roles or with other vessels, as illustrated in Figure 5. We have here also included other autonomous ships as they may have human operators further into the operation chain, maybe as supervisors at the centre or at another RCC. However, this issue is not further detailed in this paper. The figure describes an autonomous vessel in the middle, that may or may not have crew onboard, and shows the links or interaction with other vessels or control centres on shore.

Figure 5: Interaction between automation and some important human operations

Some issues that appear in this analysis are:

1. Human expectations to the automation system: How easy will it be to guess its intentions? Is the background for a decision clearly defined and presented?
2. Time for humans to gain situational awareness when automation needs to hand control over to humans, and how to guarantee that enough time is available? What kind of expertise is needed (navigation, engine, other)?
3. Times to overlap between AC and humans/operators: In some cases the T_{MR} will be too long regards the T_{DL} requirements. How can a first AC controlled action be taken before the operator is in place and can take control?
4. How can teams of operators (VTS and other ships) relate to the automation system?
5. How can an RCC be organised, with operators and experts working together? How to exchange information with other vessels and RCC's?

The operators are the backbone of the RCC. In order to assess the potential demands upon an operator, six nautical officers with a broad range of sea-going experiences and discipline expertise were recruited to contribute to the concept of developing the human-machine interfaces necessary for the RCC concept in the MUNIN project (Rødseth 2012). The research objectives were to understand how many vessels that can be operated by one operator, as well as to understand how a situation team can be allocated when needed, Hetherington (2006), Porathe (2018). Within this RCC concept, each operator was required to monitor six unmanned vessels via a monitoring and controlling workstation. Each workstation was comprised of six displays which monitors critical elements of the system. Figure 6 illustrates how this can be organised. This research had two main purposes; 1) understand the operators challenges, 2) to understand how experts in teams can be organised in a control centre.

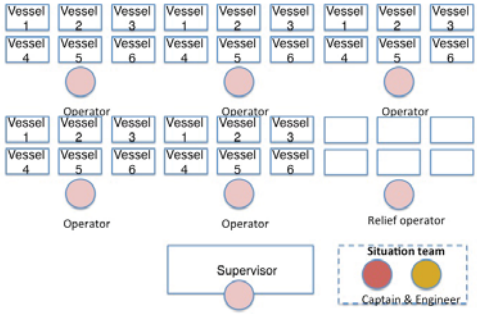

Figure 6 - RCC organisation

The overall status of the ship is simply the minimum of the indicator values for all main ship function groups. Similarly, the function group status indicator (SI) is the minimum of all function sub-group status indicators, as can be seen in Figure 7. The sum of this values will be used when estimating or defining the T_{MR} that again will address time requirements to the RCC operation.

On the final and third level, the status indicator is the minimum of the corresponding function status indicator (FSI), function condition indicator (FCI), Technical status indicator (TSI) and technical condition indicator (TCI). The FSI an FCI will normally also be accompanied by a set of characteristic data values that can further be used to see what causes non-normal flags on the FSI. The TSI and TCI may represent top-nodes in their own hierarchies or accompanied, e.g., by automation system data.

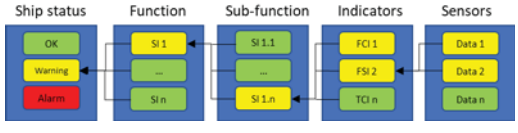

Figure 7 Principles of status aggregation

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. This because it should bring awareness to the operator. Too much detailed information could lead to an extra time constrain when a decision should be taken from a RCC. However, the message would in most cases also contain additional data values of interest, e.g., heading and distance to targets if the abnormal is related to collision avoidance as example. The status message would also contain some additional data related to the overall ship position and heading. This means that the RCC operator briefly gets an overall status assessment and without delay can assess the origin of any abnormal ship status code. This will help to ensure rapid takeover from automation to 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 needs looking at irrelevant data sets or pictures.

7 Using the operational envelope

An autonomous ship will operate in different transition levels. For each level there can be several operational envelopes of relevance, one envelope can have sub-envelopes depending on the envelopes task. When defining which envelope to use, it is also important to understand the different phases of an operation, which is explained in the bullets below and are considering operation of a MASS vessel:

- Phase O: Logistic management, voyage and load planning
- Phase 1: Carry out activities at location. This can be operations at a port, or for instance loading fish at a fish farm cage.
- Phase 2: Departure. Do the departure activities such as get acknowledgement, set operation autonomous level, and do the pre activities before sailing. This includes pilotage and route exchange.
- Phase 3: Sailing. This means the sailing between two points. A track or voyage plan must be set, and the automation level defined. It also includes interaction with traffic management (pilotage), with other vessels, with RCC, as well as status and control management during the voyage.
- Approaching destination. This includes notifications and approvals to enter destination and interact with traffic management and reporting to control centres as part of the mission.

The importance within each phase is to define whom should be in control; the automation system, operators on board the vessel, or an operator in a remote-control centre. The hand-over process between them must be clearly understood where both T_{MR} and T_{DL} is calculated. Also identification of potential hazards within each stage must be done, where fall-back procedures must be in place. In the following we will concentrate on the phase 3, sailing, where the envelope *following track* is active, see Figure 8.

Figure 8 Envelope and state diagram following track

The figure defines an envelope, the *following track envelope*, with three states, S_1 .. S_3. There will likely be other states as well, but this is only meant as an example. Each of the states depends on the parameter's *visibility,* which is visual distance in nautical miles from vessel, the *CPA* which is the Closest Point of Approach, and *TCPA* which is time to CPA i.e. the time at which CPA will happen if two ships in a collision situation maintain course and speed and are heading for an unwanted situation. Naturally a vessel will move from one state to another, and back. Fall-back, F1, is operations that happens when it leaves the envelope state, that in this case is a full stop of the vessel, which is considered as the best option if nothing else is possible.

There are different sensors in use to evaluate the ship state. For example, a camera on board the vessel can give input to the visibility. A radar or lidar can be used to define the CPA and TCPA. AIS can be an extra sensor source if radar or lidar is not in place. It is also of importance when defining the time parameters, the t_{MR} and $t_{DL,}$ to understand the technology and algorithms that have been used for the calculation. In other project, like the Integrated Maritime Autonomous Transport System, (Fjørtoft (2019)), land based or external sensors is validated to understand potentials of bringing some of the awareness from the vessel sensors to the infrastructure available along the fairway. Therefore, the T_{MR} and $T_{DL,}$ can also be calculated with the background from external sensors. It must also include calculation based on the external and internal factors mentioned in Figure 1. Another important factor is that the T_{DL} value most likely will be shorter in a high state than a low, as example in S_3 compared with S_1, since the operational window to achieve control is shorter.

Within each state presented in Figure 9 there can be many parallel processes ongoing. For example, collision avoidance will be one sub-envelope that are active during the navigation and are part of the "following track" envelope. They can also be used independently, or as part in another envelope. That means one envelope can have several sub-envelopes active, which is illustrated in Figure 9.

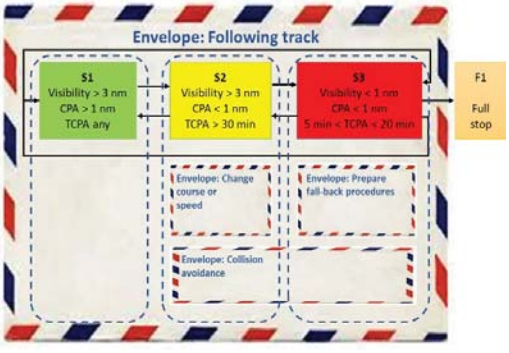

Figure 9 Envelope and state diagram following track with sub envelopes

When understanding the different envelopes and how they are connected, it is also important to understand the transition time regards handing over control from i.e. the AC to the human operators. The transition and times are calculated as a result of both internal factors, as well as external. As the example illustrates, the vessel is in the operational envelope "*following planned track*", where both internal and external factors must be included when the estimates of time or distance are calculated. If for example the MASS vessel is sailing in S_1, and a possible collision are identified as a risk and if the traffic picture does not change, it is likely that the states move in to S_2. This means we must execute the sub-envelope "*collision avoidance*" since the CPA < 1 nm. The vessel states will move further in to S_3 if the situation or potential for a conflict increases. When recovering from the situation it will move back to S_1. Again, the conditions and internal and external factors must be included when the t_{MR} and t_{DL} are estimated and calculated.

7.1 Determining critical human response requirements

Most autonomous ships will rely on a combination of automatic control and human control. This creates a potential problem in ensuring that the human has enough time to reach the control station and to gain a good enough situational awareness before an action is required. The maximum repose time t_{MR} was introduced previously to measure the time the operator needs to reach the control position and to make a decision.

Correspondingly, a formal specification of the SCT may make it possible to automatically derive a response deadline t_{DL} which is the maximum time the operator has to give a response, according to the ongoing state. To avoid that the system reverts to a minimum risk condition (MRC) through the operator exclusive states, the equation in Eq. 2 must be satisfied.

$$\forall\ s \in \boldsymbol{O}_{AC}:\ T_{MR} < T_{DL} \qquad \text{Eq. 2}$$

Deriving the T_{DL} requires that it is possible to specify times related to state transition in the SCT.

This is illustrated in Figure 10 with five main types of state transitions:

- $\boldsymbol{T_A}$**:** Transitions within the automation system's control scope.
- $\boldsymbol{T_{AO}}$*:* Transitions from automation to operator exclusive.
- $\boldsymbol{T_{AAO}}$: Transitions from automation to undetermined automation states.
- $\boldsymbol{T_{OAO}}$: Transitions from undetermined automation to operator exclusive.
- $\boldsymbol{T_F}$: Transitions from AC or operator to fall-back.

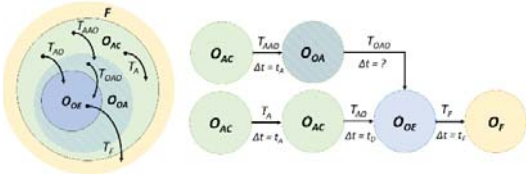

Figure 10 – State transitions and times

By comparing also with Figure 3, one will see that from a given state in $\boldsymbol{O_{AC}}$ one or more state changes are needed before the system ends up in $\boldsymbol{O_{OE}}$ and then, if the operator fails to give a response in time, the system will automatically transit to a minimum risk condition in F. The sum of times these transitions take, will together be the maximum time the operator has to respond.

One should also note that there may be more than one state transition path that ends up in an MRC for any given start state, although each path is expected to be relatively short, e.g. two to three steps as indicated in Figure 10. Given that one such path is called p and the set of all possible paths $\boldsymbol{P}$, the response deadline can be expressed as in Eq. 3.

$$\begin{aligned} p_1 &= \{(s_0, e_0, \Delta t_0), \ldots, (s_n, e_n, \Delta t_n)\} \\ \boldsymbol{P} &= \{p_1, \ldots, p_n\} \\ T_{DL} &= \min_{p \in \boldsymbol{P}} \left(\sum_{i=0}^{n} \Delta t_i\right) \end{aligned} \qquad \text{Eq. 3}$$

7.2 Using constrained autonomy

The discussion shows a problem with the $\boldsymbol{O_{OA}}$ state space: It is not possible to use transitions through that space in the calculation of the response deadline as one cannot a priori know if the automation system will be able to find a solution, or if the human is needed to resolve the problem. This can be solved in one of two ways:

1. It is possible to assign the state in $\boldsymbol{O_{OA}}$ a bounded time before it is necessary to alert the user. This would effectively move the state to $\boldsymbol{O_{AC}}$ and possibly add a new state in $\boldsymbol{O_{OE}}$.
2. The state is moved directly to $\boldsymbol{O_{OE}}$. The operator will need to supervise the automation and be ready to intervene if the automation fails to find a solution.

If this is done with all states in $\boldsymbol{O_{OA}}$ we are left with a state space containing only $\boldsymbol{O_{AC}}$ and $\boldsymbol{O_{OE}}$. This gives a deterministic deadline for all states and this is called constrained autonomy (Rødseth 2017).

In addition to giving a more deterministic response time requirements for the operator it will also improve testability of the automation system as the cases that the automation is supposed to handle is better defined.

8 Conclusions

As maritime transport organizations move to introduce autonomous vessels and develop autonomous compliant applications, many issues arise that demand considerable guidance and support in terms of robust methodologies, techniques and tools. In this paper we have outlined some of those issues and proposed certain solutions and directions towards implementing autonomous envelopes. We have also outlined several open issues regarding hand-over processes between automation, and operators, either on board a vessel or at a remote control centre ashore.

Autonomous ships will in most cases have a remote control centre (RCC) that supervises it and which can intervene when the ship ends up in situations that the automation system cannot handle by itself. The RCC will for most ships be a cost-effective and necessary component for building trustworthy autonomous ships.

However, the split of responsibilities between humans and the automation system requires a good human-automation interface (HAI) and needs careful design and analysis. The *operational envelope* has been proposed as a tool to aid in this work.

It can be used to describe what tasks that can be performed by automation and what tasks that needs human supervision or assistance. By describing this, e.g. as state machines and estimating the minimum duration of each states in a sequence that can lead to the trigger of a fall-back function, one can also estimate the minimum time the operator has to achieve controls and intervene. This is one important factor in ensuring system safety.

The analysis can also be used to detect states and events that belong in the $\boldsymbol{O_{OA}}$ category, i.e. where it is not known if the automation can handle the situations and where the minimum duration of the state cannot be assessed. These cases should be modified so that

the situation can be avoided. The resulting system can then be called "*constrained autonomous*". This is a necessary prerequisite for doing the timing analysis described above.

One may also want to add new rules for interaction between humans and automatic ships into regulations. The work can therefore be important when developing new input to existing regulative, to further increase determinism. The time constraints elaborated in this paper, as well as the hand-over process between automation and humans is likely to be address to the work when autonomous shipping is taken into consideration.

All this is work in progress that will be tested out during ongoing autonomous ship projects, among them AUTOSHIP, SAREPTA and IMAT. This paper has examined the general requirements to an operational envelope and the description of the associated tasks and have looked at some specific cases where the envelopes can be used. The studies show that the envelopes can contribute to a better and more deterministic relationship between humans and automation, where time factors are important.

9 Acknowledgements

This work has been partially funded by the Norwegian Research Council projects SAREPTA and the IMAT project. It has also received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 815012 (AUTOSHIP).

10 References

CCNR (2018). Automated Navigation – Definitions of levels of automation in inland navigation, Resolution 2018-II-16. Retrieved April 2020 from https://ccr-zkr.org/files/documents/cpresse/cp20181219en.pdf

DNV GL (2018), Class Guideline - Autonomous and remotely operated ships, DNVGL-CG-0264, September 2018.

Endsley M., (1987). "The application of human factors to the development of expert systems for advanced cockpits," in Proceedings of the 31st Annual Meeting Human Factors Society, 1987.Fjørtoft, Haugen (2019): Integrated Maritime Autonomous Systems (IMAT). ICMASS 2019.

Endsley, M. R., & Kaber, D. B. (1999). Level of automation effects on performance, situation awareness and workload in a dynamic control task. Ergonomics, 42(3).

IMO MSC/Circ.102/MEPC/Circ.392. 2002. Guidelines for Formal Safety Assessment (FSA) for use in the IMO Rule-Making Process. As amended. London: IMO 2002.

IMO COLREG; http://www.imo.org/

ISO/TR 11065:1992 Industrial automation glossary.

ISO 23860 (2019) Ships and marine technology — Terminology related to automation of Maritime Autonomous Surface Ships (MASS) – Internal Committee working draft 1, August 2019.

Grøtli, E.I., Reinen, T.A., Grythe, K., Transeth, A.A., Vagia, M., Bjerkeng, M.C., Rundtop, P., Svendsen, E., Rødseth, Ø.J. and Eidnes, G., (2015). SEATONOMY, design, development and validation of marine autonomous systems and operations. In: Proc. of the MTS/IEEE OCEANS'15, 2015.

Hetherington, C., Flin, R., & Mearns, K. (2006). Safety in shipping: The human element. Journal of safety research, 37(4), 401-411.

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

Huang, H. M., Pavek, K., Novak, B., Albus, J., & Messin, E. (2005). A framework for autonomy levels for unmanned systems (ALFUS). Proceedings of the AUVSI's Unmanned Systems North America.

Inagaki, T., & Sheridan, T. B. (2019). A critique of the SAE conditional driving automation definition, and analyses of options for improvement. Cognition, technology & work, 21(4).

Ose, Ramstad, Fjørtoft (2013), Integrated Planning and Logistics. Analysis of the logistical planning in Statoil.

Parasuraman, R., Sheridan, T. B., & Wickens, C. D. (2000). A model for types and levels of human interaction with automation. IEEE Transactions on Systems Man and Cybernetics Part A: Systems and Humans, 30(3).

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".

SAE J3016 (2016): Taxonomy and definitions for terms related to on-road motor vehicle automated driving systems, Revision September 2016, SAE International.

Sheridan, T. B., & Verplank, W. L. (1978). Human and computer control of undersea teleoperators. Man-Machine Systems Laboratory Report. Cambridge, MA: MIT.

Rødseth Ø.J. and Nordahl H. (2017), Definitions for Autonomous Merchant Ships, Norwegian Forum for Unmanned Ships, Version 1.0, 2017-10-10. Available from http://nfas.autonomous-ship.org/resources.html (Accessed December 2019).

Rødseth Ø.J (2018). Defining Ship Autonomy by Characteristic Factors, Proceedings of ICMASS 2019, Busan, Korea, ISSN 2387-4287.

Rødseth Ø.J (2018b). Assessing Business Cases for Autonomous and Unmanned Ships. In: Technology and Science for the Ships of the Future. Proceedings of NAV 2018: 19th International Conference on Ship & Maritime Research. IOS Press 2018 ISBN 978-1-61499-870-9

Rødseth Ø.J, et al (2012). Maritime Unmanned Navigation through Intelligence in Networks, D4.5: Architecture Specification. Retrieved April 2020 from http://www.unmanned-ship.org/munin/news-information/downloads-information-material/munin-deliverables/

UK Maritime (2019), Maritime Autonomous Surface Ships (MASS) UK Industry Conduct Principles and Code of Practice (2019). A Voluntary Code, November 2019. Retrieved April 2020 from https://www.maritimeuk.org/media-centre/publications/maritime-autonomous-surface-ships-industry-conduct-principles-code-practice/