CMOROC Appendix B – State of the Art

Identification of Competences for MASS Operators in Remote Operation Centres

V 2.2

Date: 25.10.2023

About this study:

This report was commissioned by the European Maritime Safety Agency (EMSA) under framework contract 2022/EMSA/OP/24/2021

Authors:

Authors	Organisation	Role
Prof. Thomas Jung	University of Appl. Sciences Bremen, Germany Institute for Maritime Simulation (IfMS)	Project lead
Dr. Marie-Christin Harre	Humatects GmbH, Oldenburg, Germany	Deputy project lead
Noelle Rousselle		Contributor
Dr. Andreas Luedtke	DLR – German Aerospace Centre Institute of Systems Engineering for Future Mobility (SE), Oldenburg, Germany	Contributor
Marcel Saager		Contributor

Recommended citation:

European Maritime Safety Agency CMOROC Identification of Competences for MASS Operators in Remote Operation Centres EMSA, Lisbon

Legal notice:

Copyright notice[1]:

---

[1] The copyright of EMSA is compatible with the CC BY 4.0 license.

Table of Contents

List of Figures

1. Introduction

This chapter offers a detailed examination of the latest advancements in Remote Operation Centres for autonomous shipping. While numerous studies, projects, and industry initiatives have been undertaken and initial outcomes have been demonstrated, our intention is not to present a comprehensive catalogue of these research endeavours. Instead, we aim to spotlight current trends, concepts, and challenges by providing a curated selection of the most pertinent projects and initiatives. The topic of remote control is relatively new in the maritime domain, thus we also investigated other domains where remote control plays a role.

In our study we use the term Remote Operation Centre (ROC). Several other terms are commonly used in the community for autonomous shipping: Shore Control Centre (SCC), Shore Operations Centre (SOC), Remote Control Centre (RCC), and Base Control Station (BCS) to name just a few. In essence, these terms refer to the same concept, a centre located onshore for monitoring and controlling one or more ships. The operators at these centres are physically separated from the ships they are monitoring and controlling. In more advanced projects (like MUNIN, LOAS), monitoring takes place during normal operation and human control is only necessary in situations that exceed or are approaching the limitations of the onboard automation. In other projects (like Seafar, FernBin), the ROC is designed for remote steering of a ship with limited automation onboard. The active involvement of human operators in both cases is crucial for the safe operation of the ships.

An important consideration in the design of ROC is how to ensure that the operator remains informed and able to intervene when necessary, or how to quickly bring her/him back in the loop when necessary.

Accepted guidelines for the design and certification of a ROC are currently missing. Therefore, early projects just replicated the ship bridge and moved it to a shore-based control centre (e.g., Dybvik, Veitch, Steinert 2020). A crucial question in this line of thinking is to what degree a level of “ship sense” must be replicated (Dybvik, Veitch, Steinert 2020): smell, sound, touch, sight, vibrations, movements. Ship sense includes for example “the experience of how a hull performs in different wave patterns”, “Risks of broaching in following seas, or slamming if you head too fast into breaking waves?” (Porathe 2021). Designers might strive to install technology to copy the same feeling a mariner would have onboard, for example using motion beds vibrating seats, and smell alarms. On the other hand, we must ask if this approach stems from a mental fixation to the old model of seafaring, and if new sensors are maybe much more reliable than the human senses (Dybvik, Veitch, Steinert 2020). Either way, it is important to recognise that the requirements for remote control differ significantly from those of direct on-board control. Some ROCs existing today realize a one-to-one relation, meaning that there is one operator directly controlling/steering one ship. In the future this will very likely not be the case. More and more autonomous ships will be approved, and one operator will be able to oversee more than one ship, at least in normal operation situations. In certain aspects, the tasks of the remote operator resemble those of Vessel Traffic Service (VTS) operators. VTS operators monitor several ships of different types. However, while VTS operators primarily monitor and assist remote ships, the remote operator in an ROC may perform direct control in certain situations. It is crucial to understand these distinctions and to define a new role for ROC operators. This role must be supported by implementing sophisticated design solutions to ensure safe and efficient operation. Developers and certification organizations are faced with new challenges when designing or approving an ROC:

- Which roles must be present in an ROC and how do they cooperate?
- Which competencies are necessary for these roles?
- How many ships can be monitored by an operator at the same time?
- How to support an adequate situational awareness via the human-machine interaction (what information, when, in what form), and how to compensate for not being on-board the ship?
- When should operators in the ROC take manual control?
- How do legal aspects influence the design of an ROC?
- How to design robust cybersecurity measures to protect against potential cyber-attacks that could compromise the safety and operation of the ship?
- Will ROCs be operated by ports, by shipping companies, by VTS centres, or by private companies?
- Will there by different ROC for different parts of the voyage with associated hand-over procedures?
- Will one ROC be able to operate very different types of ships?

In this report, we present selected projects/initiatives, and we show how these challenges have been addressed. Each project below has been analysed according to the following questions:

- Which automation use cases are investigated?
- How is the ROC structured and organised?
  This includes workstations, operator roles, cooperation, tasks, HMI.
- How have safety and security for ROCs been addressed?
- Which legal aspects have been considered?

At the end of each project, we summarise statements and findings which are used to guide the other steps in the CMOROC study. Statements and findings are derived considering the following categories: (Category C1) principal elements of MASS and MASS ROC, (Category C2) technical requirements on MASS ROC, (Category C3) requirements on human-interaction in MASS ROC, and (Category C4) legal requirements on MASS ROC.

The report starts with an overview on two previous EMSA studies (SAFEMASS and RBAT) which are relevant for CMOROC study. Next the Code of Practice by Maritime UK is presented as an example of regulations for MASS. Afterwards maritime research and industrial projects as well as projects from other domains are analysed.

2. Previous EMSA Studies

EMSA commissioned two studies on Maritime Autonomous Surface Ships (MASS), which are highly relevant for the CMOROC study:

- SAFEMASS: Study of the risks and regulatory issues of specific cases of MASS
- RBAT: Risk Based Assessment Tool

Both studies where contracted to DNVGL (www.dnv.com). The objectives and main results will be described in the following.

2.1 SAFEMASS - Study of the risks and regulatory issues of specific cases of MASS

SAFEMASS (July 2019 – March 2020) identified emerging risks and regulatory gaps that are entailed by the introduction of MASS. In particular, two levels of autonomy are considered according to IMO (2018):

- A3-B1: Autonomous with qualified operators on board.
    - A3: The qualified operator is informed by the system in case of emergency or when ship systems are outside of defined parameters. Permission of the qualified operator is not required for the ship system to execute functions, decisions and actions; the qualified operator can override the ship system when outside of defined parameters. Provided the boundaries of the ship systems are not exceeded, “human control” becomes “human supervision”.
    - B1: Qualified operators on board

- A2-B0: Supervised without qualified operators on board.
    - A2: The qualified operator is always informed of all decisions taken by the systems. Permission of the qualified operator is not required for the ship systems to execute functions, decisions and action; the qualified operator can override the systems at any stage.
    - B0: No qualified operators on board but qualified operators available at a remote location

The study results report consists of two main parts (plus a summary part). Part 1 (European Maritime Safety Agency 2020a) focusses on emerging risks arising from ships with A3-B1 level of autonomy whereas Part 2 focusses on A2-B0.

The autonomy level A3-B1 in Part 1 allows less personnel onboard and also longer periods with an unmanned bridge. In Part I monitoring and control from a remote location, such as a control centre located onshore have been excluded. As use cases three different types of vessels are examined conceptually: a short route domestic passenger ship, a short-sea cargo ship and an ocean-going cargo ship.

From the perspective of the three use cases a hazard identification (HAZID) and a fault tree analysis (FTA) have been performed. Based on the results risk control options (RCO) and measures (RCM) have been suggested. Additionally, existing regulations have been analysed and challenges with regard to A3-B1 autonomy have been pointed out.

The HAZID in particular considered "human-in-the-loop" challenges. The human operators on board can be out of the loop for longer periods of time. But when system limits are reached or in emergency cases the operators might have to intervene and take over. In such cases the system has to support the operators in gaining a sufficient situation awareness quickly.

As a preparation for the HAZID generic functions and sub-functions involved in A3-B1 were identified, which resulted in a generic function tree. Because of the importance of the human element for each function the role of the operator in performing the function was defined according to the following four categories:

- "Detection: Acquisition of information that is relevant for the control of a function. The information may be based on sensors and/or human perceptions."
- "Analysis: Interpretation of the acquired information into a situational understanding relevant for the control of the function."
- "Planning/ decision-making: Determination of needed changes in control parameters in order to keep the function performance within the applicable frames."
- "Action: Effectuating the planned changes of control parameters, typically via actuators operated via a control system. This is however considered to be conventional systems based on existing technologies, accordingly this report assumes this part is handled by existing safety regimes."

In the HAZID, hazards, causes and consequences have been identified. In a subsequent Fault Tree Analysis (FTA). The FTA explores the causal relationship between events which singly or in combination contribute to the occurrence of a higher-level hazardous event.

Based on the HAZID and FTA specific issues with regard to human-in-the-loop have been highlighted. Three categories have been considered: not being able to build up situational awareness (SA), mode confusion and (dis-)trust in automation. For each of these categories human-related risks have been identified and documented.

Five risk control options (RCO) have been identified:

- RCO #1 – Ensure robust communication between MASS and other vessels.
- RCO #2 – Ensure that MASS operator(s) are capable of mustering at the bridge when required.
- RCO #3 – Ensure that task unfamiliarity and complexity does not impair human performance.
- RCO #4 – Ensure sufficient levels of system redundancy and reliability in MASS design and operations.

In Part 2 (European Maritime Safety Agency 2020b.) the autonomy level A2-B0 is investigated using the same methodology as in Part 1. A2-B0 involves operation from a remote centre, thus the functional analysis includes function of an ROC. Again human-related risks have been highlighted, which involves "capacities and abilities required to supervise multiple vessels in various operational modes, incl. in case of abnormal situations and emergencies.":

- "Human-machine interfaces (HMI) and other visual displays required for successful acquisition and analysis of information, decision-making and implementation of control actions."
- "Threats to operator vigilance induced by human factors such as boredom or underload during quiet and normal operations, as well as stress and other negative factors present during periods with high workload."
- "Influence from challenges with communication link, such as latency and connectivity."
- "Operators' diminished ship sense from being remotely located (onshore), e.g., reduced or altered perceptions of stability, speed, heading and environmental conditions."
- "Challenges related to not being physically present to fix problems, e.g., in case of maintenance, equipment failures or rescue operations."

Four risk control options (RCO) have been identified:

- RCO #1 – Ensure sufficient reliability of systems performing navigation functions.

- RCO #2 – Ensure sufficient reliability of ROC operators’ response actions to system failures.
- RCO #3 – Ensure sufficient supervision capacity and availability of ROC.
- RCO #4 – Ensure sufficient capability for MASS fleet to enter minimum risk conditions.

In summary, the study stresses the importance of considering the interaction between humans and automation. In particular, the following general suggestions are pointed out:

- Potential “ironies of automation”- pitfalls should be avoided.
- Principles of human-centred design should be adopted.
- Human Factors Engineering techniques and standards should be applied.
- Automation should be considered at a task and system function level, supported by definitions and models which allow more nuanced evaluations of joint human-system interactions.
- Demands imposed on the human operators have to be considered when designing function allocation between human and machine.
- The human element should be considered already early in the design stage when defining the MASS Concept of Operations (ConOps).

2.2 RBAT - Risk Based Assessment Tool

RBAT started in 2020 and was still ongoing at the time of preparation of this state-of-the-art report (2023). The objective was to develop and test a Risk-Based Assessment Tool (RBAT) for maritime autonomous surface ships (MASS).

The RBAT methodology consists of five main parts (European Maritime Safety Agency 2023): (i) Describe use of automation (and remote control), (ii) perform hazard analysis, (iii) perform mitigation analysis, (iv) perform risk evaluation, (v) address risk control.

- Part 1: Describe use of automation (and remote control)
    - Step 1: Describe the vessel's mission (operational goals)

      A mission consists of an overall mission goal like “Safe and timely transport of cargo from one Port X to Port Y”, the mission phases, which are “typically characterized by a recognizable shift in where the vessel is located in terms of geographical surroundings, or the start and end of one or more operations like “Arrival in port” and the operations, which are “activities performed as part of a mission phase in order to achieve the mission goal”, like “Perform docking”.

    - Step 2: Describe the automated and/or remotely controlled functions (functional goals)

      Control functions, which serve to perform operations, and the control actions, which serve perform the control function are described. Together step1 and 2 results into a hierarchical goal structure (Figure 1):

- Mission: Safe and timely transport of cargo from Port X to Port Y
    - Mission phase: Arrival in port
        - Operation: Perform docking
            - Control function: Perform manoeuvring
                - Control action Y: Adjust speed
                - Control action Z: Adjust heading

Figure 1: Example of a hierarchical goal structure

    - Step 3: Describe how control functions are allocated to agents.

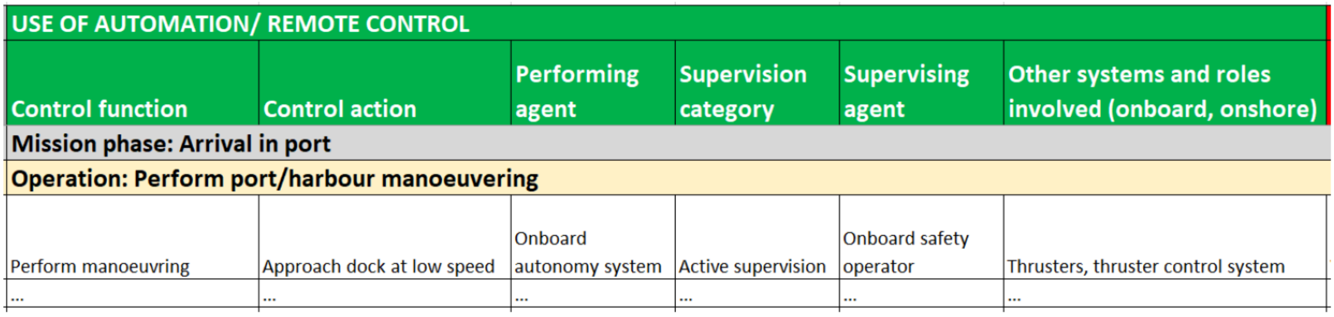
It is defined whether a function is performed by humans or machines. Additionally, the geographical location is indicated: “R” for Remote and “O” for onboard (vessel),

- Step 4: Assign responsibility for supervision of control actions.

  There are four types of supervision:

  - Active (human) supervision: a human agent continuously monitors the performance of a control action and intervenes when necessary.
  - Passive (human) supervision: a human agent is monitors the performance of a control action and successfully intervene when requested by the system.
  - Machine supervision: a machine agent continuously8 monitors the performance of a control action and intervenes when necessary.
  - No supervision.

  The results of 3 and 4 are documented using a table like the one in Figure 2



USE OF AUTOMATION/ REMOTE CONTROL					
Control function	**Control action**	**Performing agent**	**Supervision category**	**Supervising agent**	**Other systems and roles involved (onboard, onshore)**
Mission phase: Arrival in port					
Operation: Perform port/harbour manoeuvering					
Perform manoeuvring	Approach dock at low speed	Onboard autonomy system	Active supervision	Onboard safety operator	Thrusters, thruster control system
...	...	...	...	...	...

Figure 2: Automation table

- Part 2: Perform hazard analysis.
  - Step 5: Identify unsafe conditions/modes associated with control actions.

    For each control action from step 2 conditions are identified where “a system is operating outside its normal (and safe) operating envelope due degraded performance (e.g., failures) or exceeding its capabilities which, if left unmitigated, has the potential to cause an accident (i.e., losses)”. For this purpose, guidewords as shown in are applied.

Unsafe conditions/modes	Guidewords
Not providing the control action leads to a hazardous event	Not provided
Providing the control action leads to a hazardous event	Provided when not required
	Incapable/not fit for purpose
Incorrectly provided control actions leads to a hazardous event	Control parameters out of range
	Control parameters are within range but incorrect
	Too early/late or in wrong of order
	Stops too soon
	Applied too long
Control action not being followed leads to a hazardous event	Not followed/Rejected

Figure 3: Unsafe condition/mode guidewords

- Step 6: Identify causal factors which may initiate the unsafe conditions/modes.

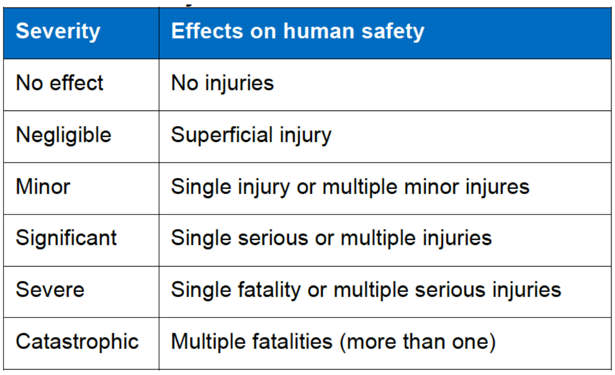
  Internal failures or insufficient capabilities for dealing with external hazards are identified as potential causal factors for unsafe conditions. The following failure categories are considered: random (hardware) failures, systematic failures, systemic failures, operator failures, failures due to environmental conditions, failures due to deliberate actions.

- Step 7: Describe the worst-case outcomes from (unmitigated) unsafe conditions/modes.

  Worst-case outcomes are identified and categorises according to the following accident categories: No effect on safety, Injuries/loss of life (general), Loss of control, Collision, Contact, Damage to/ loss of ship equipment, Hull failure, Fire/explosion, Grounding/stranding, Capsize/listing, Flooding/foundering, non-accidental event, Missing vessel.

- Step 8: Rank the worst-case outcomes severity.

  The worst-case outcomes from step 7 are ranked according to severity index the shown in Figure 4.



Severity	Effects on human safety
No effect	No injuries
Negligible	Superficial injury
Minor	Single injury or multiple minor injures
Significant	Single serious or multiple injuries
Severe	Single fatality or multiple serious injuries
Catastrophic	Multiple fatalities (more than one)

Figure 4: Severity index

- Part 3: Perform mitigation analysis.
  - Step 9: Nominate mitigation layers which can prevent losses.

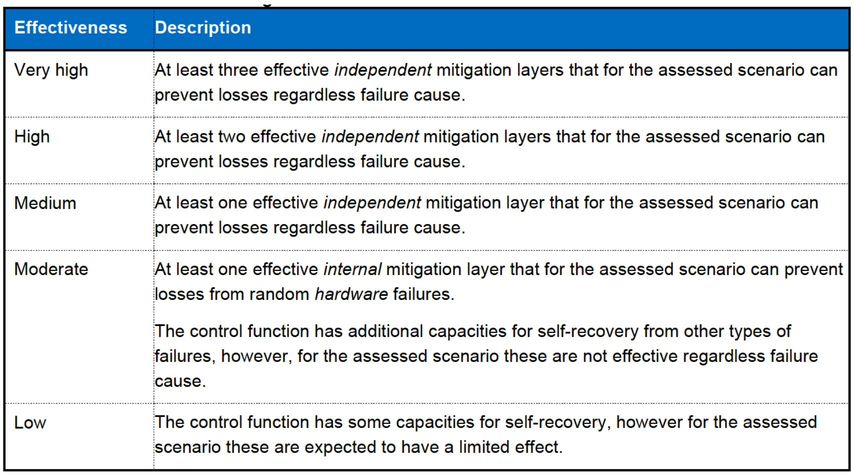
    In this step, self-recovery capacities and potential are identified and described: Applicability of the mitigation layer, system and human involvement in the mitigation layer, limitations to the mitigation layer, transitions between and from mitigation layers (including minimum risk conditions)

  - Step 10 Qualify the nominated mitigation layers.

    The effectiveness of the mitigation layers from step 9 is evaluated against the following criteria: Functionality, integrity, robustness, independence, human involvement.

  - Step 11: Rank the mitigation layers effectiveness.

    The mitigation layers are ranked according to their effectiveness using the categories shown in Figure 5.



Effectiveness	Description
Very high	At least three effective *independent* mitigation layers that for the assessed scenario can prevent losses regardless failure cause.
High	At least two effective *independent* mitigation layers that for the assessed scenario can prevent losses regardless failure cause.
Medium	At least one effective *independent* mitigation layer that for the assessed scenario can prevent losses regardless failure cause.
Moderate	At least one effective *internal* mitigation layer that for the assessed scenario can prevent losses from random *hardware* failures. The control function has additional capacities for self-recovery from other types of failures, however, for the assessed scenario these are not effective regardless failure cause.
Low	The control function has some capacities for self-recovery, however for the assessed scenario these are expected to have a limited effect.

Figure 5: Effectiveness of mitigations

- Step 12: Perform prevention analysis (optional)

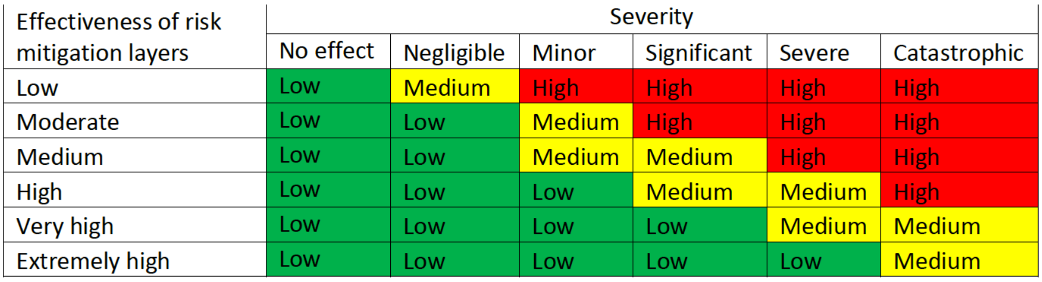
  In addition to mitigation, in this step existing measures to prevent the occurrence of unsafe condition should be identified. This includes “maintenance, testing and inspection for technical equipment, or rules about operational restrictions”.

- Part 4: Perform risk evaluation.

  - Step 13: Determine risk level for each assessed scenario.

    The risk level is assessed for each risk scenario: Causal factor -> unsafe condition/ mode -> mitigation layers -> worst-case outcome. The severity and the effectiveness of risk mitigation layers should be identified using the categories shown in. The “as low as is reasonably practicable” (ALARP) principle should be applied:

    - “High (red region): Risk cannot be justified and must be reduced, irrespectively of costs.”
    - “Medium (yellow ALARP region): Risk is to be reduced to a level as low as is reasonably practicable.”
    - “Low (green region): Risk is negligible, and no risk reduction is required.”



Effectiveness of risk mitigation layers	Severity					
	No effect	Negligible	Minor	Significant	Severe	Catastrophic
Low	Low	Medium	High	High	High	High
Moderate	Low	Low	Medium	High	High	High
Medium	Low	Low	Medium	Medium	High	High
High	Low	Low	Low	Medium	Medium	High
Very high	Low	Low	Low	Low	Medium	Medium
Extremely high	Low	Low	Low	Low	Low	Medium

Figure 6: Risk matrix based on evaluation of available risk mitigating measures

  - Step 14: Alternative justifications for determining risk levels.

    In some cases, it might be reasonable to assume lower risk levels. In order to explore this, the following arguments should be investigated:

    - “Operational restrictions such as speed limits and weather restrictions.”
    - “Exposure rate to the relevant hazard.”
    - “If the initiating event14 is not related to software, it may be possible to argue for a lower probability than what has been generally anticipated for control functions.”

    - “It should be possible to argue that a single mitigation will increase the effectiveness of the mitigation by more than one level.”
    - “It should also be possible to demonstrate that safety critical control functions performing more complex functionality than emergency stop has a better performance”.

- Part 5: Address risk control
  - Step 15: Identify and document risk control measures.

    Decisions are made for risk control measures. These should be documented adequately. Risks can be reduced by:

    - Updating the design.
    - Removing or reducing the hazard associated with the control function.
    - Introduce operational restrictions which reduces the hazards potential impact.
    - Improving the control functions integrity (and thus reducing its failure frequency).

3. Code of Practice by Maritime UK

Currently, international rules for the certification of MASS and ROCs do not exist. In 2017, the IMO (International Maritime Organisation) started a scoping exercise to determine how MASS can be regulated and to which degree safety, security, and environmentally sound operation of MASS is addressed through the existing IMO instruments. This exercise was completed in 2021 by the IMO’s Maritime Safety Committee (MSC). The final report (IMO 2021) describes how the existing regulatory framework is affected by MASS, identifies themes and/or potential gaps, and provides guidelines for future updates of the regulations.

The MSC approved interim guidelines for the conduction of MASS trials (IMO 2019). The document lists ten key elements to be considered for the planning and conducting of trials: Risk management, compliance with mandatory instruments, manning and qualification of personnel, the human element, infrastructure, trial awareness, communication and data exchange, reporting requirements and information sharing, scope and objective for each individual trial, and cyber risk management. These elements shall provide guidelines to coastal States, flag States and port States to give approval to MASS trials within their own territorial waters. In principle, a MASS must follow the international regulations established by the international bodies, mainly the International Maritime Organization just like any other vessel (Safari, Sage 2013).

Maritime UK (2018) published The Code of Practice (the Code) for operation of MASS in UK inland and coastal waters. Maritime UK is an industry organisation encompassing the UK’s shipping, ports, services, engineering, and leisure marine industries. The Code describes requirements for software on board and in an ROC. Furthermore, the organisation of an ROC is specified. The Code of Practice provides a good basis to understand the regulatory framework to which MASS and ROC developers must comply, thus a short overview of chapters relevant for the study shall be provided.

The Code of Practice (the Code) has been prepared by the UK Maritime Autonomous Systems Working Group (MASRWG), and provides practical guidance, sets initial standards and best practice for the design, construction, and safe operation of MASS under 24 meters. To get a certificate, the MASS must comply with all the requirements of the Code of Practice. A certificate is issued for a particular area of operation.

3.1 Which automation use cases are investigated?

Ship:	MASS which are to be registered in the United Kingdom, specifically those less than 24 meters in length.
Level of automation:	A MASS with every different level of control

Route/Area:	Within the United Kingdom or United Kingdom waters (at sea and/or inland waters).

3.2 How is the ROC structured and organised?

Within the Code, an ROC is referred to as Base Control Station (BCS). The BCS is responsible for the tasks:

- Operation Planning,
- Operation Control, and
- Post Operation Analysis.

The Code provides an example for a BCS organisation (responsibility diagram, Figure 7). In this example, the BCS is on board of a mother ship. The example includes five roles for the BCS:

1. Master/Commanding Officer:
    - Overall responsibility for the ship and her crew, and all operations including those involving off board systems (MASS);
    - Authorises the mission plan.
2. Watch Officer
    - Manages and commands the complete MASS mission;
    - Manages the interaction between MASS BCS operator, crane operator, payload operators, etc;
    - Involved in mission planning, execution, and post mission evaluation;
    - Direct communication with equipment operators;
    - If the MASS Watch Officer (MWO) is located in the Operations Room, then the oversight of crane/deck operations will pass to the commanding officer on the bridge.
3. BCS Operator:
    - Receives commands from the Watch Officer;
    - Responsible for the MASS command and control when operated by the BCS;
    - Responsible for mission planning, execution, and post mission evaluation;
    - Could be fully or partially responsible (shared with payload operator) for launch and recovery of vehicle payloads (ROVs, AUVs, towed systems);
    - Likely to communicate with other operators, e.g., crane operator, secondary operator on deck, and payload operators.
4. Ship Crane Operator:
    - Receives commands from the Watch Officer;
    - Responsible for lifting and lowering MASS to/from water;
    - Will require communication with the MASS BCS and MASS secondary operator on deck as appropriate.
5. MASS Payload Operator:
    - Receives commands from the Watch Officer;
    - Could receive commands directly from the MASS BCS Operator;
    - Responsible for operation of payload;
    - Could be fully or partially responsible (shared with BCS operator) for launch and recovery of vehicle payload (ROVs, AUVs, towed systems);
    - Will have communication with MASS BCS Operator;
    - This role could be conducted by the BCS Operator.
6. Additionally, the BSC team must include a MASS Security Officer (MSO)

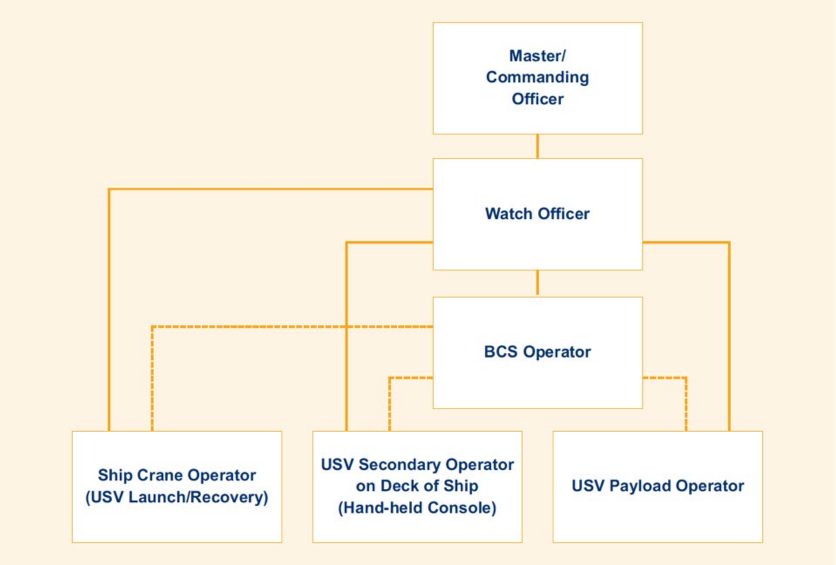


Figure 7: Example of a responsibility diagram for a BCS, copied from Maritime UK (2018).

The Code states that the operator in a BCS must be provided with sufficient data to assess and to react to requests. A list of example data and requests is given:

- Health Status of MASS, including warnings and alerts:
    - Built in Test Equipment (BITE) data presented to BCS;
    - Battery status;
    - Fuel level;
    - Engine or equipment condition and performance warnings;
    - Fire on-board.
- MASS navigational data:
    - Actual position, Heading, CoG, SoG;
    - Planned course.
- MASS requests:
    - Request to perform some form of action that requires BCS authorisation.
- Situational Awareness data within the vicinity of MASS, for example:
    - Target/obstacle Track Data;
    - Camera data;
    - Radar data;
    - In water sensor data (e.g., obstacle avoidance sonar);
    - Sound data (e.g., warnings from other vessels).
- Collision Avoidance:
    - Warnings of potential obstacles.
    - MASS intended action (autonomy level dependent)
- Attack or interference with the MASS or its subsystems.
- Chart overlays, including land mass, shipping lanes, charted obstacles, seabed topography (if required).

Finally, a list of operational requirements for a BCS is provided. Examples for these requirements are:

- The BCS should enable the operator to take direct control of the MASS at any time;
- The BCS should alert the operator of any changes to the planned mission, such as change in speed, heading, or collision avoidance manoeuvres;
- The BCS should be easy to use. The types of information displayed should be based on the priority of importance. Safety related warnings, graphical or audible, should be displayed on the Graphical User Interface (GUI), regardless of the GUI configuration.

3.3 How have safety and security for ROCs been addressed?

The Code states that a hazard identification and a risk assessment shall be performed. The chosen method (e.g., Failure Modes and Effects Analysis) shall be applied to the MASS systems, sub-systems, and components, and to the operation of the MASS. The failure probability shall be quantified, e.g., probability per 10,000 hours of operation.

It has to be shown that the MASS and its operation is as safe as an equivalent manned ship.

The MASS has to be equipped with adequate failure sensors to detect and mitigate risks. The BCS operator shall be alerted of any emergency warnings or a change in condition with regard to immanent risk. Clear conditions have to be defined for an emergency stop, meaning that propulsion is reduced to a safe level in a timely manner.

The risk assessment has to clearly point out the failure modes, installed failure sensors, and the chosen mitigation measures. These will be a crucial basis for the accreditation of the MASS.

In addition to the risk assessment, a specific security assessment shall be performed including the MASS and the BCS. The assessment should include:

- Identification of existing security measures, procedures, and operations with respect to both physical and cyber intrusion.
- Identification and evaluation of critical MASS and shore-based operations that it is important to protect.
- Identification of possible threats, both physical and cyber, to the key MASS operations, and the likelihood of their occurrence in order to prioritise security measures.
- Identification of weakness, including human factors, in the infrastructure, policies, and procedures.

The MASS must be equipped with a Security Alert System, which communicates security events to a competent authority. Additionally, there should be a mechanism for safely shutting down MASS communications in case of security events involving the BCS.

The security measures must be set out in a MASS Security Plan that includes for example:

- Measures to prevent dangerous substances being taken on board the MASS or into its control station;
- Identification of the restricted areas and measures for the prevention of unauthorised access to those areas, both on the vessel and in the MASS control station;
- Measures to prevent unauthorised access to restricted areas on the vessel or at the control station, e.g.:
    - controlling access to the MASS itself and to its control station;
    - controlling the boarding of persons on the MASS;
    - monitoring restricted areas of the MASS control station to ensure that only authorised persons have access.
- Procedures for responding to threats of security breaches, including provisions for maintaining critical operations of the MASS or, as the case may be, shutting them down;
- Duties of shore-based personnel assigned security responsibilities;
- Procedure for ensuring, testing, calibration, and maintenance of security equipment on the MASS and that located in the control station;
- Frequency for testing, calibration and maintenance of security equipment on the MASS and that located in the control station.

3.4 Which legal aspects have been considered?

In order to test and certify a MASS and its BCS, the risk assessment as well as the cyber security analysis shall be reviewed in detail. It must be checked that all critical single point failures have been considered. The risk mitigation measures must reduce the risk to an acceptable low level.

All failure modes shall be individually tested by simulating each failure and by verifying that the backup measures are effective in mitigating any critical consequences. The Code suggests using simulators, but in cases where real-world stimuli are essential to test certain functions (e.g., optical and inertial sensors), real-world trials have to be performed.

3.5 Statements and Findings

For our study, the following statements and findings have been derived from the Code of Practice:

Nr.	Statement / Finding	Source	Categories
SoA-CP-1	Six roles for an ROC are suggested: Master/Commanding Officer, Watch Officer, ROC Operator, Ship Crane Operator, MASS Payload Operator, MASS Security Officer	Code of Practice (Maritime UK)	C1
SoA-CP- 2	The ROC should provide the following data: Health status of MASS (including warnings and alerts), MASS navigational data, MASS requests, situational awareness data within the vicinity of MASS, collision avoidance, attack or interference with the MASS or its subsystems, chart overlays, including land mass, shipping lanes, charted obstacles, seabed topography.	Code of Practice (Maritime UK)	C3
SoA-CP-3	The ROC should enable the operator to take direct control of the MASS at any time.	Code of Practice (Maritime UK)	C2, C3
SoA-CP-4	The ROC should alert the operator of any changes to the planned mission, such as change in speed, heading, or collision avoidance manoeuvres.	Code of Practice (Maritime UK)	C2, C3
SoA-CP-5	The type of information displayed should be based on the priority of importance.	Code of Practice (Maritime UK)	C3
SoA-CP-6	Safety related warnings, graphical or audible, should be displayed on the Graphical User Interface (GUI), regardless of the GUI configuration	Code of Practice (Maritime UK)	C3
SoA-CP-7	A risk assessment and a security assessment must be performed.	Code of Practice (Maritime UK)	C4
SoA-CP-8	The MASS should be equipped with adequate failure sensors to detect and mitigate risks.	Code of Practice (Maritime UK)	C2
SoA-CP-9	Clear conditions should be defined for an emergency stop.	Code of Practice (Maritime UK)	C2
SoA-CP-10	The MASS should be equipped with a Security Alert System	Code of Practice (Maritime UK)	C2
SoA-CP-11	Basis for certification should be the risk assessment, the cyber security analysis, simulator tests, and real-world trials.	Code of Practice (Maritime UK)	C4
SoA-CP-12	For certification, it must be checked that all critical single point failures have been considered.	Code of Practice (Maritime UK)	C4

4. MUNIN (European Project, 7th Framework Programme)

Project name:	Maritime Unmanned Navigation through Intelligence in Networks
Runtime:	2012 - 2015
Website:	www.unmanned-ship.org/munin/
Consortium: Fraunhofer CML (Germany), MARINTEK (Norway), Chalmers (Sweden), Hochschule Wismar (Germany), aptomar AS (Norway), MarineSoft (Germany), Marorka ehf (Iceland), University College Cork (Ireland) t	

Objective: Develop “a technical concept for the operation of an unmanned merchant ship and assess its technical, economic, and legal feasibility.”

4.1 Which automation use cases are investigated?

Ship:	Dry bulk carrier operating in intercontinental tramp trades.
Level of automation:	Autonomous ship without seafarers on-board during deep-sea legs of the voyage; a pilot enters the ship to take control outbound or inbound from port.
Route/Area:	Deep-sea voyage; congested of restricted waters are not considered for autonomous control.

4.2 How is the ROC structured and organised?

In MUNIN, the term Shore Control Centre (SCC) is used. The project had a special focus on the SCC and the design is described in detail in several publications. A design for an operator workstation equipped with six screens for monitoring six ships at the same time is suggested (Figure 8). The screens of the operator workstation provide the following information (Porathe 2014):

- Dashboard: The top middle screen provides 145 information items grouped in nine information panels for each of the six ships (on the right), and an indication of the current automation mode of the ships (the circle on the left). The panels show information e.g., about the voyage, sailing, security, cargo etc. Each panel will have a coloured flag as the top indicator: green, yellow, or red. Yellow indicates that the ship needs special attention e.g., because some values exceed pre-set thresholds, but the situation is non-critical. Red indicates critical deviations. The automation modes on the right indicate for example, if the ship is under autonomous control, under SCC’s remote control, fail-to-safe mode, or manual control onboard.
- Bottom middle screen: If a certain ship needs special attention, the operator can put it here to investigate the details of the nine information panels. Figure 9 provides an overview of the structure of the 145 information items that can be explored to monitor a ship and to find deviations from thresholds. More details on the structure and information items can be found in MUNIN Consortium (2015).
- Spatial overview: This screen shows an ECDIS-like (Electronic Charts Display and Information System) display with overlayed information illustrating ship limitations in form of turning radiuses and the “safe heaven”, which depicts the planned position of the ship (cf. Figure 10). The overlay provides a “visual understanding of upcoming events”.
- Temporal overview: This screen provides a temporal view on the whole voyage of a ship broken down into days or, if zoomed in, into hours (cf. Figure 11). It shows the voyage in the time zone of the ship and the time zone of the SCC. The timeline indicates events which require the operator to perform actions like sending a message to the pilot.
- Ship status indicator: This indicator (cf. Figure 12) shows the time to maintenance in comparison to time to destination for the top-level ship system down to subsystems and further down to individual components. The hierarchy level for the displayed status can be changed using the slider on the left.
- Trendlines are used to compare a timeline of a certain parameter value (e.g., engine values) with a past timeline of the same parameter. This can be used to detect anomalies or to extrapolate the current value into the future.

Figure 8: HMI of the operator workstation, copied from MUNIN Consortium (2015).

It is assumed that an operator spends 10 minutes with each ship, checking relevant parameters via the dashboard in a repetitive monitoring cycle. In this cycle, each ship is considered once every hour.

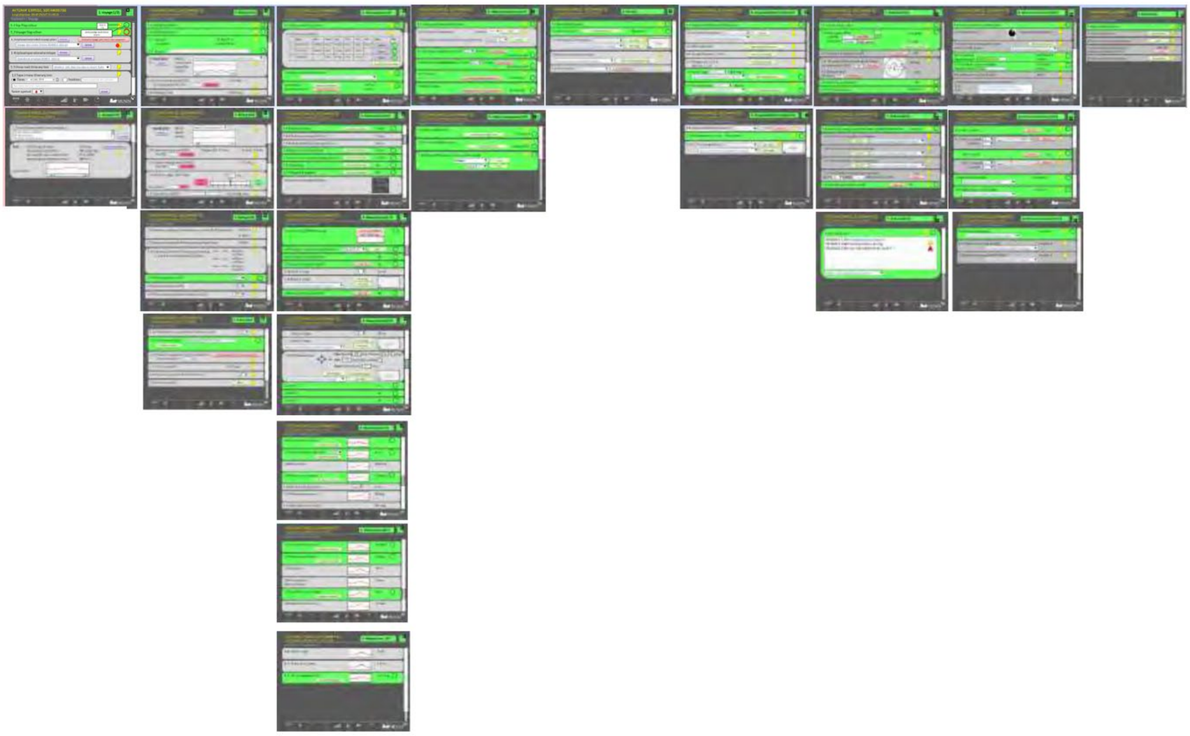


Figure 9: Overview on the structure of information available for each ship, copied from MUNIN Consortium (2015).

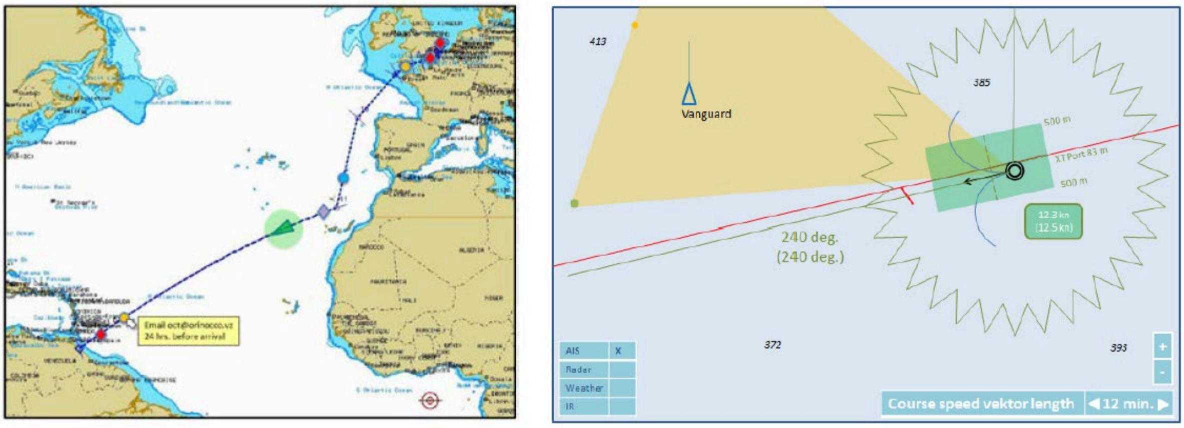


Figure 10: ECDIS-like display for spatial overview (left) and zoom in (right) on egocentric information on a specific ship, copied from Porathe (2014).

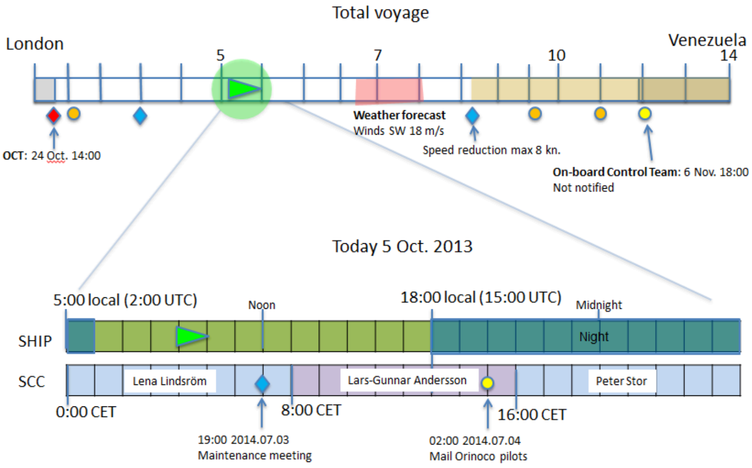


Figure 11: Temporal overview of the voyage of a ship, copied from Porathe (2014).

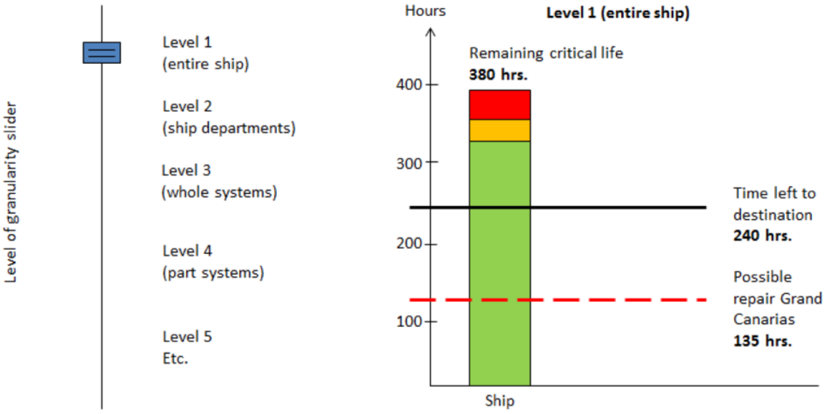


Figure 12: Ship status indicator time to maintenance in comparison to time to destination, copied from Porathe (2014).

Remote control can be performed from a Remote Manoeuvring Support System (RMSS). The RMSS supports navigation by showing predicted ship trajectories. These predictions are computed based on the engine parameters using fast-time simulation.

The MUNIN project elaborates on staff organisation of the SCC (MacKinnon, Man, Baldauf 2015). This organisation as shown in Figure 13 foresees four roles:

- SCC Operator: has a navigational background and monitors six ships by observing high-level and low-level information via a corresponding dashboard HMI for each ship. In case of emergency, they cooperate with their supervisor, captain, and engineer, and provide information about the ship in order to get these actors in the loop quickly.
- SCC Supervisor: (re-)allocates resources e.g., by deciding when to involve the captain and engineer.
- SCC Captain: is the head of the SCC and takes legal responsibility. Together with the operator in charge they perform remote ship handling if needed, from the situation handling room using the Remote Manoeuvring Support System (RMSS).
- SCC Engineer: provides technical knowledge and expertise to solve problems with onboard equipment.

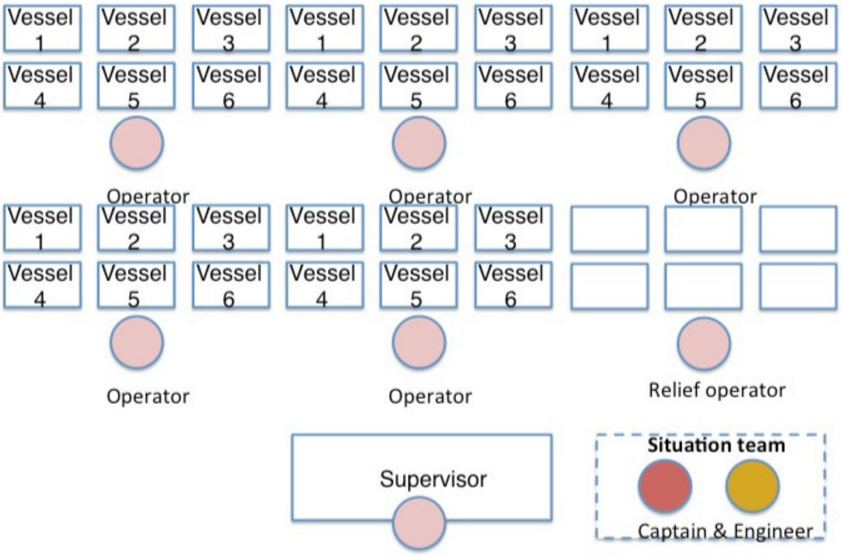
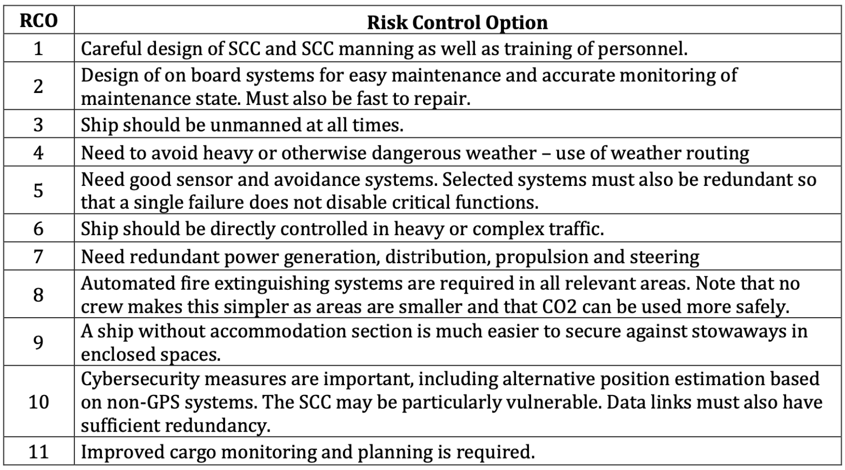


Figure 13: Organisation of the SCC in MUNIN, copied from MacKinnon, Man and Baldauf (2015).

4.3 How have safety and security for ROCs been addressed?

Generic hazards and risks for unmanned shipping have been identified in workshops with subject matter experts (Kretschmann et al. 2015). 23 hazards have been identified for which risk control measures are needed. 11 risk control option have been defined as shown in Figure 14.



RCO	Risk Control Option
1	Careful design of SCC and SCC manning as well as training of personnel.
2	Design of on board systems for easy maintenance and accurate monitoring of maintenance state. Must also be fast to repair.
3	Ship should be unmanned at all times.
4	Need to avoid heavy or otherwise dangerous weather – use of weather routing
5	Need good sensor and avoidance systems. Selected systems must also be redundant so that a single failure does not disable critical functions.
6	Ship should be directly controlled in heavy or complex traffic.
7	Need redundant power generation, distribution, propulsion and steering
8	Automated fire extinguishing systems are required in all relevant areas. Note that no crew makes this simpler as areas are smaller and that CO2 can be used more safely.
9	A ship without accommodation section is much easier to secure against stowaways in enclosed spaces.
10	Cybersecurity measures are important, including alternative position estimation based on non-GPS systems. The SCC may be particularly vulnerable. Data links must also have sufficient redundancy.
11	Improved cargo monitoring and planning is required.

Figure 14: Generic risk control option, copied from Kretschmann et al. (2015).

4.4 Which legal aspects have been considered?

An analytical study of the main issues to be solved regarding legal aspects has been performed (Safari, Sage 2013). It focused on collision, maintenance, lookout, and watchkeeping:

- Collision: when there is no crew on board, the SCC takes over all obligations and responsibilities to prevent a collision. The SCC must make sure that a safe speed is determined, and that radar equipment (if fitted) is used properly. The following factors have to be taken into account (Safari, Sage 2013): 1) state of visibility, 2) traffic density including concentrations of fishing vessels or any other vessels, 3) manoeuvrability of the vessel with special reference to stopping distance and turning ability in the prevailing conditions, 4) at night the presence of background light such as from shore lights or from back scatter of the vessels's own lights, 5) the state of wind, sea and current, and the proximity of navigational hazards, 6) draft in relation to the available depth of water. With regard to the use of radar, specific consideration has to be given to the characteristics, efficiency, and limitations. The SCC should also have knowledge about other systems for communication and navigational like ECDIS, AIS, GNSS, and ARPA. The SCC must take any positive action in sufficient time, and the action must be apparent to another vessel.
- Maintenance: The SCC must monitor and control shore-based maintenance. At sea, maintenance and the necessity of repairs should be detected by the systems on board and should be reported to the SCC.
- Lookout: The role of a lookout may be taken over by systems on the autonomous ship, but the SCC must contribute to situations that are challenging with regard to state of weather and sea, traffic density, or traffic separation schemes.
- Watchkeeping: The systems on board the autonomous ship should detect areas of limited visibility. The exact assessment of the visibility data must be done by the SCC. The SCC must be ready to take appropriate actions in situations of limited visibility.

4.5 Statements and Findings

For our study the following statements and findings have been derived from the MUNIN project:

Nr.	Statement / Finding	Source	Categories
SoA-MU-1	A display with a hierarchical information presentation for the ship status (including for example voyage, sailing, security, cargo) is suggested. The status can be shown on the top level using coloured flags.	MUNIN	C3
SoA-MU-2	A spatial overview providing a visual understanding of upcoming events is suggested.	MUNIN	C3
SoA-MU-3	A display providing a temporal view on the whole voyage is suggested.	MUNIN	C3
SoA-MU-4	A display showing the time to maintenance in comparison to time to destination is suggested.	MUNIN	C3
SoA-MU-5	Trendlines for critical parameters are suggested to detect anomalies or to extrapolate the current value into the future.	MUNIN	C3
SoA-MU-6	Four roles for an ROC are suggested: ROC Operator, SCC Supervisor, SCC Captain, SCC Engineer	MUNIN	C1
SoA-MU-7	11 risk control options are suggested (see Appendix B)	MUNIN	C2
SoA-MU-8	The ROC must make sure that a safe speed is determined, and that radar equipment (if fitted) is used properly.	MUNIN	C4
SoA-MU-9	In addition to Radar, the ROC should have knowledge about systems for communication and navigation, like ECDIS, AIS, GNSS, and ARPA.	MUNIN	C4
SoA-MU-10	The ROC must monitor and control shore-based maintenance.	MUNIN	C4

SoA-MU-11	At sea, maintenance and the necessity of repair should be detected by the systems on board and should be reported to the SCC.	MUNIN	C4
SoA-MU-12	The role of a lookout may be taken over by systems on the autonomous ship, supported by the ROC in challenging situations.	MUNIN	C4
SoA-MU-13	The systems on board the autonomous ship should detect areas of limited visibility, while the exact assessment of the visibility data must be done by the ROC. The ROC must be ready to take appropriate actions in situations of limited visibility.	MUNIN	C4

5. H2H (European Project, Horizon 2020)

Project name:	Hull to Hull
Runtime:	2017 – 2021
Website:	www.sintef.no/projectweb/hull-to-hull
Consortium: Kongsberg Seatex (Norway), SINTEF Ocean (Norway), SINTEF Digital (Norway), Mampaey Offshore Industries (The Netherlands), KU Leuven (Belgium)	
Objective: “To develop a concept demonstrating hull to hull positioning between two vessels or between shore and vessel. The concept will support safe navigation in close proximity of other vessels and objects, being stationary or moving. H2H will assist mariners in making correct navigation decisions. Further, H2H technology will be essential in the development of autonomous vessels.” (Hull to Hull Consortium, 2018)	

5.1 Which automation use cases are investigated?

Ship:	Self-propelled barge (the Cogge), length 4.81 m, beam 0.63 m, maximal draft 0.35 m
Level of automation:	Remotely controlled
Route/Area:	Inland Waterways, Yser river

5.2 How is the ROC structured and organised

In H2H the ROC is called Inland Shore Control Centre (I-SCC) (Peeters et al. 2020). Peeters et al. (2020) state four requirements for their design of the I-SCC:

1. The needed information should be communicated in the form of information groups: sailing, observations, safety and emergencies, security, and technical.
2. The I-SCC should provide means to remotely control the ship motion and its system configurations.
3. Industrial, marine-grade components should be used for the design of the I-SCC.
4. The system design should be modular and flexible to allow future extensions.

Figure 15 shows the I-SCC realised in H2H:

- 33, 34, 35: The Bow Display, Starboard Display, and Port Display show a live stream of a 180° view of the ship’s surroundings.
- 36: Monitor information and monitor computer. The authors do not provide further details about the presented information.

- 39: Two azimuth controllers for steering the ship. The H2H ship (the Cogge) has a propulsion system with two embedded 360-degrees-steerable thruster systems, one positioned at the bow and one positioned at the stern.
- 38: A computer (programmable logic controller) that processes the steering commands from the azimuth controllers (39) and sends them via a 3G mobile internet connection to the onboard computer.
- 40: A motion control touch screen displaying data for steering the ship. The display shows the current internal steering angles, the propeller speeds for both actuators, and the values from the azimuth controllers as adjusted by the operator.

The main information provided to the controller are the video streams which provide a 180 ° view of the ship surrounding. The operator can steer the ship via the azimuth controllers.

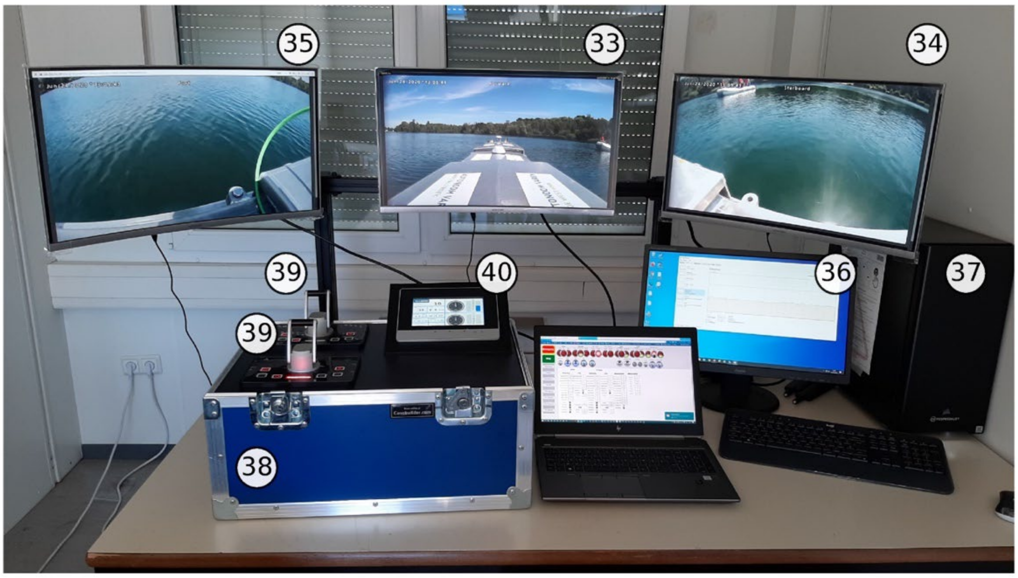


Figure 15: I-SCC realised in H2H for remote control of the Cogge, copied from Peeters et al. (2020).

5.3 How have safety and security for ROCs been addressed?

In line with requirement 3. from above (Section 5.2), industrially robust components have been selected to reduce the risk (Peeters et al. 2020). Furthermore, multiple interaction possibilities with the vessel and onboard safety stops have been installed.

5.4 Which legal aspects have been considered?

Myhre, Rødseth, and Petersen (2020) define a method that allows the use of legal aspects as a starting point of the design process. In their method they suggest using accountability "as a basis for systems design of autonomous and remote-controlled operations." Figure 16 shows their 3 + 3 step method.

In phase 1, an accountability concept is defined and the overall requirements for the technical design of this concept are derived. In phase 2, a top-level system design is developed that realises the requirements from phase 1.

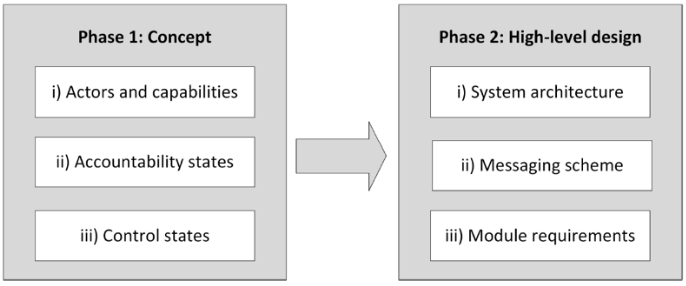


Figure 16: 3 + 3 step method to use accountability as a starting point for system design, copied from Myhre, Rødseth, and Petersen (2020).

In the following, the 3 + 3 steps are briefly described. The authors use a simple theoretical use case to illustrate their method: an uncrewed autonomous ship that is able to navigate autonomously in open sea under supervision of a remote operator.

- Phase 1 - Actors and capabilities. The actors and their capabilities are defined. The use case involves four actors: (see Figure 17)
    - Navigation & Control unit (N&C): sends commands to the physical actuators of the ship in order to steer the vessel and to regulate speed.
    - Autonomous Ship Controller (ASC): is able to autonomously compute navigation commands that are sent to the N&C.
    - Minimum Risk Condition unit (MRC): computes navigation command for a minimum risk manoeuvre and sends corresponding commands to the N&C.
    - ROC Operator (ROCO): monitors the ship and can send commands to the N&C via a wireless connection.

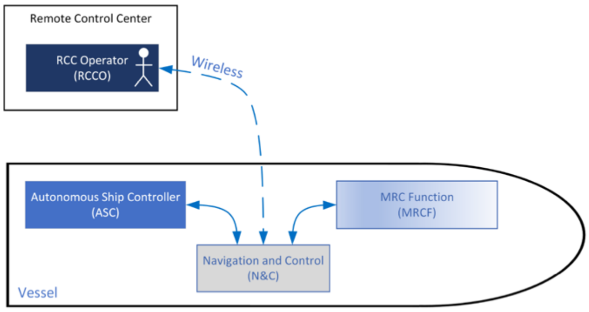


Figure 17: Actors for the theoretical use case., copied from Myhre, Rødseth, and Petersen (2020).

- Phase 1 - Accountability States: It is defined which actor is accountable in which conditions and how accountability can be transferred (see Figure 18).
    - In port, the ROCO is accountable.
    - During the sea passage, the ROCO can hand over accountability to the ACC if explicitly accepted by the ACC.
    - The ROCO can reclaim accountability at any time.
    - When the MRC is active, the accountability stays with the ROCO.
    - The ACC will not automatically hand over the accountability when the ship approaches a port. Instead, the ROCO has to recognize the situation and has to actively reclaim accountability.

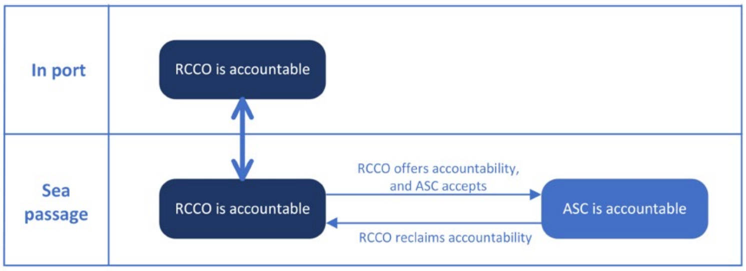


Figure 18: Accountability diagram, copied from Myhre, Rødseth, and Petersen (2020).

- Phase 1 - Control States: It is defined which component has control over the ship under which conditions. To have control means that the components send commands to the N&C. Control should be clearly defined at any point in time. The control logic is shown in Figure 19.

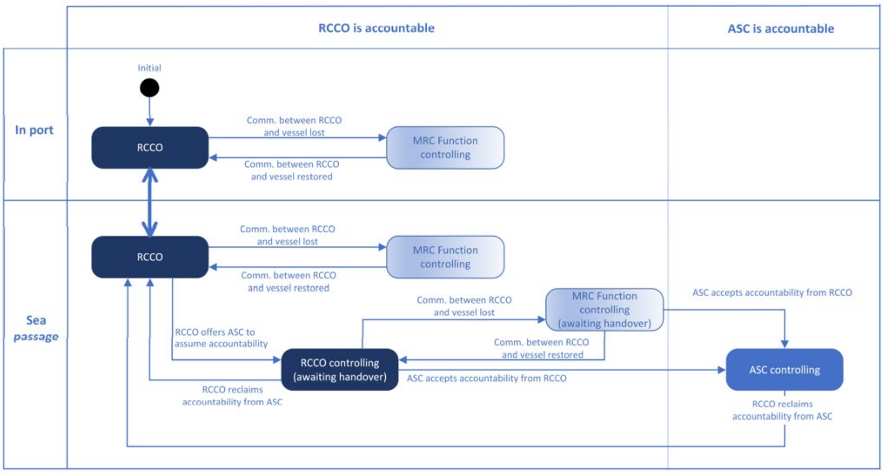


Figure 19: Control state diagram, copied from Myhre, Rødseth, and Petersen (2020).

The authors derived the following high-level design requirements:

- “Initially, the ROCO holds accountability and thus provides input to N&C.”
- “If the ROCO provides input to N&C and communication between ROCO and the vessel fails, then the MRC Function shall provide input to N&C.”
- “If the MRC Function provides input to N&C and communication between the ROCO and the vessel is restored, then the ROCO shall provide input to N&C.”
- “While in sea passage, the ROCO may offer ASC to assume accountability.”
- “If, and only if, the ROCO has offered ASC to assume accountability, ASC may accept (or implicitly refuse, by not accepting) the offer for accountability.”
- “If ASC accepts accountability, ASC shall provide input to N&C.”
- “If ASC provides input to N&C, the ROCO may at any time reclaim accountability. If the ROCO reclaims accountability, the ROCO shall provide input to N&C.”
- “The ROCO may at any time withdraw an offer to ASC of assuming accountability. This equals to reclaiming accountability from ASC.”

- Phase 2: A system architecture is designed that fulfils the requirements. Additionally, a messaging system is defined for communication between the components. Finally, the requirements are derived for the implementation of the individual modules of the architecture.

5.5 Statements and Findings

For our study the following statements and findings have been derived from the H2H project:

Nr.	Statement / Finding	Source	Category
SoA-HH-1	The needed information should be communicated in the form of information groups: sailing, observations, safety and emergencies, security, and technical.	H2H	C3
SoA-HH-2	The system design should be modular and flexible to allow future extensions.	H2H	C2
SoA-HH-3	Three displays showing a live stream of a 180° view of the ship's surroundings are suggested: Bow Display, Starboard Display, and Port Display.	H2H	C3
SoA-HH-4	A motion control touch screen displaying data for steering the ship is suggested.	H2H	C3
SoA-HH-5	A method for using accountability as a basis for system design of autonomous and remote-controlled operations is suggested.	H2H	C4

6. AUTOSHIP (European Project, Horizon 2020)

Project name:	Autonomous Shipping Initiative for European Waters
Runtime:	06/2019 – 11/2023
Website:	www.autoship-project.eu

Consortium:
Ciaotech S.r.l. – PNO Group (Italy), Kongsberg Maritime AS, Norway, Kongsberg Digital AS (Norway), Kongsberg Norcontrol AS, Norway, Sintef Ocean AS, Norway, University of Strathclyde (Scotland), Eidsvaag AS (Norway), ZULU Associates (Belgium), Bureau Veritas (France), DE VLAAMSE WATERWEG NV (Belgium)

Objective:
Building and operating 1) two vessels with full-autonomous navigation, self-diagnostic, prognostics, and operation scheduling, 2) a ROC, and 3) a communication infrastructure, which includes means for cyber security. The targeted TRL is 7 and beyond. Additionally, digital tools and methodologies for design, simulation, and cost analysis are developed.

6.1 Which automation use cases are investigated?

Use Case A:

Ship:	Catamaran (ZULU 4), a class2 pallet shuttle barge, up to 350 t of goods
Level of automation:	Remotely controlled ship without seafarers on board
Route/Area:	Inland water ways, operating in the Flemish region around the port of Antwerp

Use Case B:

Ship:	Cargo ship, 1,462 deadweight capacity (DWT), 74.7 m length
Level of automation:	Remotely controlled ship without seafarers on board
Route/Area	Short sea shipping, transporting fish feed from the factories of Skretting and Cargill to fish farms along the Norwegian coast, sailing between Hirtshals in Denmark and Kristiansand in Norway.

6.2 How is the ROC structured and organised?

The ROC in AUTOSHIP has the following functions (Bolbot et al. 2020a):

- monitoring of physical processes,
- navigation control,
- control over the ship in emergency/manoeuvring operating modes,
- implementation of software updates.

Figure 20 shows the laboratory setup of the AutoShip Remote Operation Workstation (AutoShip consortium 2022). In March 2023, when the state-of-the-art report was prepared, more information on the structure and organisation of the ROC could not be found. Since AutoShip was still running at that time, more information was expected to be released later in 2023.

Figure 20: Remote Operation Workstation from the AutoShip project, copied from AutoShip consortium (2022).

6.3 How have safety and security for ROCs been addressed?

The method for risk assessment in the AutoShip project (Bolbot et al. 2021) is based on the guidelines for autonomous shipping published by Bureau Veritas (2019). It consists of seven steps:

- Step 1 - Use case description: The use cases is described by defining for example, the main parameters of the ship, the ship autonomy, the manning level, the operating area and limitations, the financial input, the infrastructure, the power and propulsion setup, and the ship functions and systems.
- Step 2 - Selection of function groups for analysis: The functions on which the analysis shall be focused are selected. These are in general those functions with a higher level of autonomy compared to non-autonomous ships.
- Step 3 - Identification of hazards, causes, and consequences: Hazards are identified by following the process in Figure 21. A crucial step is the identification of inadvertent events. This is done by applying so called guide words to the output of a specific function. Guide words are for example: “provided wrong”, “not provided”, “provided in timely”, “provided results in conflict”.
- Step 4 - Identification of risk control measures: In order to be able to mitigate the identified hazards, potential risk control measures are identified. Potential categories of such measures are the following: “a) designing out risk, b) using safety devices, c) applying fault tolerance techniques, d) operational procedures and training, e) avoiding risk, f) sharing risk.”

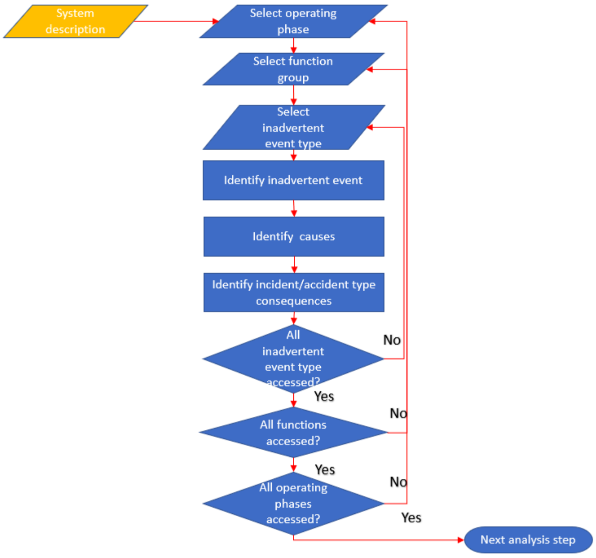


Figure 21: Hazard identification process, copied from Bolbot et al. (2021).

- Step 5: Risk review and risk index estimation: To compute the risk of hazards, numbers for frequency (Figure 22) and severity (Figure 23) are assessed by subject matter experts in a workshop. Agreed numbers are derived from individual assessment by computing an average. Risk is computed by adding the average numbers for frequency and severity.

Ranking (FI)	Frequency	Definition	F (per ship year)	F (per ship hour)
7	Frequent	Likely to occur once per month on one ship	10 (5–50)	$1.14\ 10^{-3}$
5	Reasonably probable	Likely to occur once per year in a fleet of 10 ships, i.e. likely to occur a few times during the ship's life	10^{-1} ($5\ 10^{-2}$– $5\ 10^{-1}$)	$1.14\ 10^{-5}$
3	Remote	Likely to occur once per year in a fleet of 1,000 ships, i.e., likely to occur in the total life of several similar ships	10^{-3} ($5\ 10^{-4}$–$5\ 10^{-3}$)	$1.14\ 10^{-7}$
1	Extremely remote	Likely to occur once in the lifetime (20 years) of a world fleet of 5,000 ships.	10^{-5} (0– $5\ 10^{-5}$)	$1.14\ 10^{-9}$

Figure 22: Ranking for frequency assessments, copied from Bolbot et al. (2021).

		Safety	Environmental			Financial	Reputation
Ranking (SI)	Severity	Effects on human Safety	Oil spillage definition	Air pollution	Other e.g. for ballast water treatment failures or collision with animals	Effect from ship operation disruption / court costs / insurance costs / fines / Effect on ship	Effect on company reputation
5	Catastrophi	Multiple fatalities (1-10 and more)	Oil spill size between 100 and 1000 tonnes	Major air pollution with long-term environmental consequences	Impact such as persistent reduction in ecosystem function or significant disruption of a sensitive species	\$80,000,000 (>\$25,000,000) Total loss	Extensive negative attention in international media/industry
4	Severe	Single fatality or multiple severe injuries. Full recovery with extensive medical treatment	Oil spill size between 10 and 100 tonnes	Air pollution resulting in air evacuation	Impact such as significant widespread and persistent changes in habitat, species or environment media	\$8,000,000 (\$2,500,000 ~\$25,000,000) Severe damage	National impact and public concern; Mobilisation of action groups
3	Significant	One or more injuries, not severe. Full recovery with medical treatment	Oil spill size between 1 and 10 tonnes	Limited environmental impact due to air pollution involving reporting to authorities	Impact such as localised but irreversible habitat loss or widespread, long-term effects on habitat, species or environmental media	\$800,000 (\$250,000 ~ \$2,500,000) Non-severe ship damage	Considerable impact; regional public/slight national media attention
2	Minor	One or more first-aid injury. Treatment is minimal or not necessary.	Oil spill size < 1 tonne	Limited to no air pollution	Impact such as localised, long-term degradation of sensitive habitat or widespread short-term impacts to habitat, species or environmental media	\$80,000 (\$25,000 –\$250,000) Local equipment damage	Limited impact; local public concern may include media
1	Negligible	Minor first-aid injury to a single person in the workforce. Treatment is minimal or not necessary.	Non-significant spill	Minor environmental impact	Impact such as localised or short-term effects on habitat, species and environmental media	\$8,000 (<\$25,000) No damage	Slight impact; local public awareness, but no public concern

Figure 23: Ranking for severity assessments, copied from Bolbot et al. (2021).

- Step 6 - Selection of risk control measures and fail-safe procedures: Risk control measures are selected considering the rankings from Step 5. For all of the identified hazards, fail-safe procedures are identified. Possible procedures are shown in Figure 24.

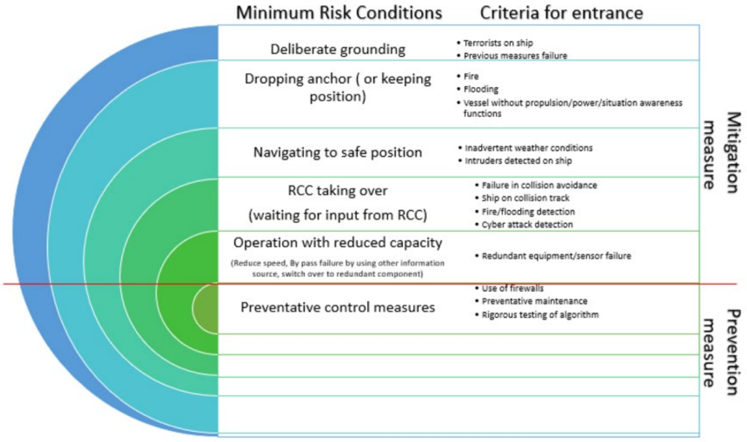


Figure 24: Fail-safe procedures, copied from Bolbot et al. (2021).

- Step 7 - Writing and revising the deliverable: The results of the risk analysis are documented in a deliverable.

Additionally, a new method for identification and assessment of cyber security for autonomous ships has been devised in AutoShip: CYber-Risk Assessment for Marine Systems (CYRA-MS, see Bolbot et al. 2020b). It consists of ten steps grouped in four phases as shown in Figure 25:

- Phase A. In this preliminary phase, the main elements to be further investigated in the next phases are identified: the control system elements with their functions and interfaces (sensors and actuators) with the physical world, the controlled processes, the interfaces among the control systems, the data flow in the system, the potential entry points into the system (physical and logical access points), different groups of attackers, and known vulnerabilities.
- Phase B. For each of the items and hacker groups identified in phase A, potential attack types and potential consequences (safety, environmental, financial) are identified and described as scenarios.
- Phase C. The scenarios are ranked according to their expected likelihood and severity. Since statistical data is currently missing for cyber-attacks on autonomous ships, the authors suggest to assess the likelihood based on the following influence factors: the level of exposure of each system to attacks due to the connectivity and complexity level, the interest of the specific attack group in an attack scenario, the attacker technological level, each attack group activity level, the ease of exploitation, the vulnerability level due to the absence/presence, as well as the effectiveness of mitigating and preventative barriers for each scenario.
- Phase D. Non-acceptable risks are selected, and appropriate mitigation measures are identified to reduce the risk. The authors consider avoiding risk (e.g., changing the operational area), removing the risk source (e.g., reducing the connectivity level), influencing the likelihood (e.g., adding control barriers), mitigating the consequences (e.g., enhancing the response and recovery after attack), and sharing risk through insurance as mitigation measures.

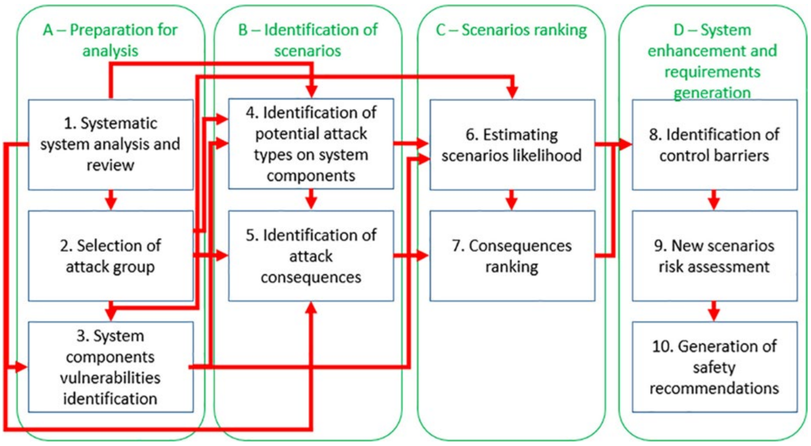


Figure 25: CYber-Risk Assessment for Marine Systems (CYRA-MS), copied from Bolbot et al. (2020b).

The new methodology is applied to the fully autonomous version of the Pallet Shuttle Barge (use case A, described above) focussing on the vessel navigation and propulsion systems. As a result, the system architecture shown in Figure 26 has been devised. It consists of four network zones based on the means of communication. The ROC is situated in Zone 1. The architecture implements the following security barriers (Bolbot et al. 2020b, 2020a):

- secure network for communication between vessel and shore control centre,
- no communication with the public network,
- two or three factors authentication for software updates and patching,
- encryption for the VHF signals,
- firewalls and redundant communication lines with different technologies for communication between the network zones,
- Zone 2 includes an intrusion detection system that monitors for system safety and suspicious controller behaviour,
- sanity checks and filter applications are implemented for the GPS signal measurements,
- plan route verification by the shore control centre,
- selecting critical health sensor measurements and sending them to the shore control centre at specific intervals,
- anti-interference antennas to reduce the impact of the GPS signal loss,
- autonomous ship controller, intrusion detection system, and navigation system operate in a kernel function to prevent installing software without permission.

.

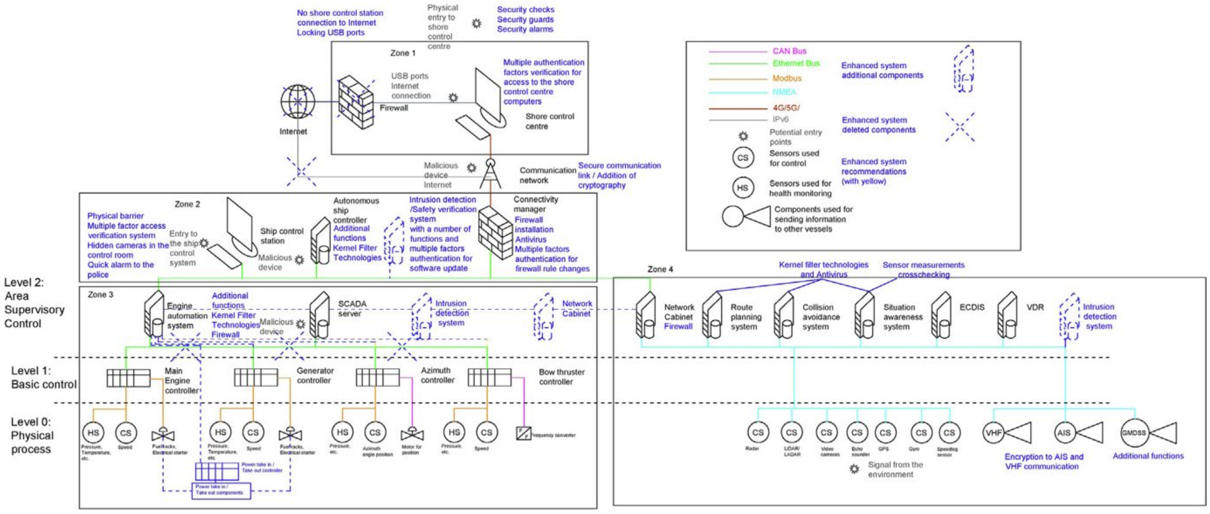
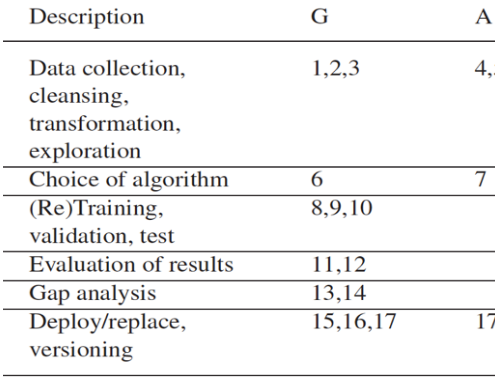


Figure 26: Zone-based logical network with security barriers, copied from Bolbot et al. (2020b).

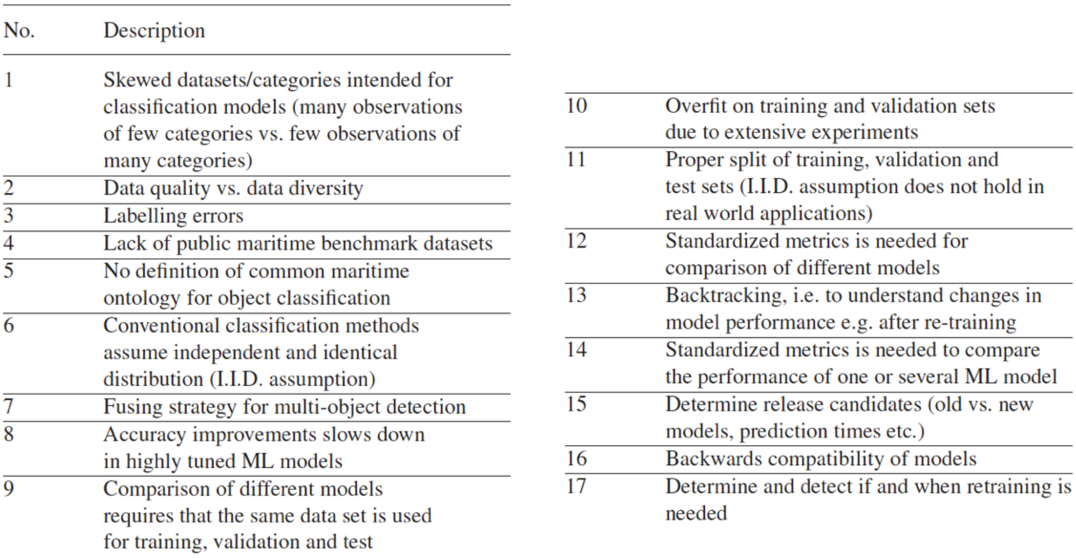
6.4 Which legal aspects have been considered?

In AUTOSHIP, guidelines for the approval of AI-based systems in autonomous shipping have been derived. The project investigates Artificial Intelligence (AI) for a Situation Awareness System (SAS) and for an Autonomous Navigation System (ANS) (Murray et al. 2022). Challenges for the development of approvable AI have been identified. The project considers models like artificial neural networks that are learned based on data using machine learning techniques. The challenges have been allocated to the different steps in the machine learning process. The steps of the development process are shown in Figure 27. The challenges for each step are shown in Figure 28.



Description	G	A
Data collection, cleansing, transformation, exploration	1,2,3	4,
Choice of algorithm	6	7
(Re)Training, validation, test	8,9,10	
Evaluation of results	11,12	
Gap analysis	13,14	
Deploy/replace, versioning	15,16,17	17

Figure 27: Steps of a machine learning process with associated challenges. Numbers refer to Figure 28. “G” means generic challenges, “A” means application specific challenges. Copied from Murray et al. (2022).



No.	Description
1	Skewed datasets/categories intended for classification models (many observations of few categories vs. few observations of many categories)
2	Data quality vs. data diversity
3	Labelling errors
4	Lack of public maritime benchmark datasets
5	No definition of common maritime ontology for object classification
6	Conventional classification methods assume independent and identical distribution (I.I.D. assumption)
7	Fusing strategy for multi-object detection
8	Accuracy improvements slows down in highly tuned ML models
9	Comparison of different models requires that the same data set is used for training, validation and test
10	Overfit on training and validation sets due to extensive experiments
11	Proper split of training, validation and test sets (I.I.D. assumption does not hold in real world applications)
12	Standardized metrics is needed for comparison of different models
13	Backtracking, i.e. to understand changes in model performance e.g. after re-training
14	Standardized metrics is needed to compare the performance of one or several ML model
15	Determine release candidates (old vs. new models, prediction times etc.)
16	Backwards compatibility of models
17	Determine and detect if and when retraining is needed

Figure 28: Challenges for the AI systems considered in the AUTOSHIP project, copied from Murray et al. (2022).

Because of these challenges and the resulting limitations of AI systems, AUTOSHIP points out that the approval of AI should not focus on the core functionality of the AI alone (e.g., object identification), but should consider its ability to recognize its own limits as well as solutions for handing over control to a human operator including solutions to bring the operator back into the loop (Murray et al. 2022).

The AI should be able to assess the certainty/uncertainty of, for example, its object identification. If uncertainty is “too high”, the operator must be informed and prepared to take over. Uncertainty can be high in situations for which no or too little training data or data with a high level of variance was available during the model development process.

Solutions for human-machine interaction are needed to bring the operator back in the loop when the AI-model reaches its limits. A crucial part this process is that the AI must be able to provide explanations of its reasoning. The decisions of the AI must be transparent and understandable for the operator. AUTOSHIP stresses the point that techniques allowing inspection of the model (like guided backpropagation) are not sufficient. Explanation of the reasoning behind the model predictions must be related to the operator’s domain knowledge.

In order to formalise the limits of the AI or automation, AUTOSHIP suggest using the concept of an Operational Design Domain (Rødseth, Lien Wennersberg, Nordahl 2022). The Operational Design Domain (ODD) stems from the Automotive Domain. In the Automotive Domain, the ODD specifies the conditions (e.g., roadway types, speed range, weather) for which an automated car is designed to operate. AUTOSHIP extends this concept towards considering the dynamic sharing of responsibilities between automation and human operators. This means that the

Maritime ODD defines how humans and automation operate a ship collaboratively, including the dynamic allocation of tasks in varying circumstances.

The intention of the Maritime ODD can be compared to the operation envelop which is a part of the Concept of Operations (ConOps) that is required in several regulatory guidelines. But while the ConOps requires specification of the particular geographic area and the specific operations for which the automation shall be approved, the Maritime ODD is more general and is supposed to cater for approval of autonomous ship systems in several geographic areas and several operations that share the conditions defined in the ODD.

A central element of the Maritime ODD is a functional mapping that allocates the responsibilities for the execution of ship control tasks (e.g., track and speed control, object detection and classification, obstacle avoidance) to human operators and/or automation. This distribution of task responsibilities can be formalised using UML. Figure 29 shows an example of an UML state diagram for shared control between automation and ROC operator for ship navigation.

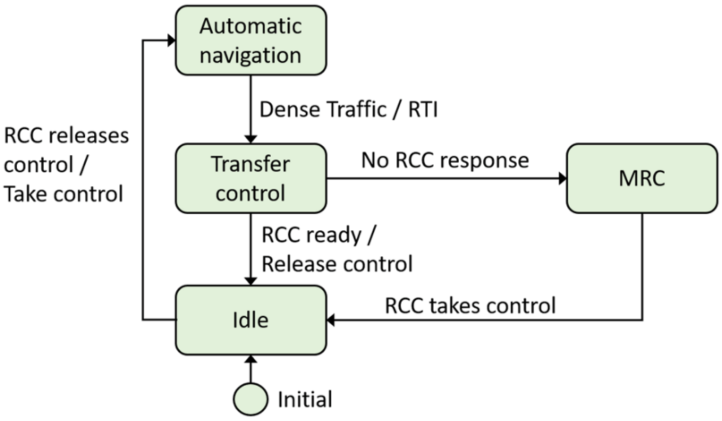


Figure 29: Example of an UML state diagram for formalisation of the Maritime ODD, copied from Rødseth, Lien Wennersberg and Nordahl (2022).

6.5 Statements and Findings

For our study the following statements and findings have been derived from the AutoShip project:

Nr.	Statement / Finding	Source	Category
SoA-AS-1	A method for risk assessment based on the guidelines for autonomous shipping published by Bureau Veritas is suggested.	AutoShip	C4
SoA-AS-2	Six fail-safe procedures are suggested.	AutoShip	C2
SoA-AS-3	A method for cyber risk management is suggested.	AutoShip	C4
SoA-AS-4	A system architecture to address security issues is suggested. It consists of four network zones (based on the means of communication) with security barriers between them.	AutoShip	C2
SoA-AS-5	The approval of Artificial Intelligence (AI) should not focus on the core functionality of the AI alone but should consider its ability to recognise its own limits as well as solutions for handing over control to a human operator including solutions to bring the operator back into the loop.	AutoShip	C4
SoA-AS-6	The decisions of the Artificial Intelligence (AI) must be transparent and understandable for the operator. Explanation of the reasoning behind the AI model predictions must be related to the operator's domain knowledge.	AutoShip	C3

SoA-AS-7	In order to formalise the limits of the Artificial Intelligence or automation, the concept of an Operational Design Domain (ODD) formalised in the form of UML diagrams is suggested.	AutoShip	C4

7. AVATAR (European Project, Interreg North Sea Region)

Project name:	Autonomous vessels, cost-effective transhipment, waste return
Runtime:	05/2020 – 06/2023
Website:	https://northsearegion.eu/avatar
Consortium: POM Oost-Vlaanderen (Belgium), Logistics Initiative Hamburg (Germany), KULeuven (Belgium), University of Oldenburg (Germany), Opleidingscentrum voor Hout en Bouw vzw (Belgium), E. Van Wingen NV (Belgium), TUDelft (Netherlands), SEAFAR (Belgium), SSPA Sweden AB (Sweden), Urban Waterway Logistics (Belgium)	
Objective: “The AVATAR project aims to tackle challenges of city freight distribution by developing, testing, and assessing adequate technologies and business models for urban autonomous zero-emission Inland Waterway Transport (IWT) solutions.”	

7.1 Which automation use cases are investigated?

Ship:	Ship 1: Catamaran (Maverick), 1 tonne vessel Ship 2: a newly built vessel with a capacity of approx. 25 tonnes
Level of automation:	Remotely controlled
Route/Area:	Canals in Ghent, Leuven, Delft, and Hamburg

7.2 How is the ROC structured and organised?

In AVATAR, an ROC architecture was defined by the University of Oldenburg which allows remote control of one or more ships from the shore side (Lamm, Piotrowski, Hahn 2022). This architecture is specifically designed to support situational awareness of human ROC operators. To achieve this, the functional components have been mapped to the three levels of situation awareness as defined by Endsley (1995):

- Perception: to perceive values of items in the environment.
- Comprehension: to interpret perceived values with regard to their impact on own objectives.
- Projection: to predict the future status and action of items in the environment.

A specific architectural level is foreseen for each of the situational awareness levels:

- Level 1: A sensor system provides data about the state of the environment and navigational information (e.g., ship position, course, speed, heading, rate of turn, nautical charts, radar, weather warnings) and the internal state of the vessel (e.g., engine, rudder, thruster, cargo). This data is presented on the Vessel Information Display.
- Level 2: The data is compared to predefined limits to automatically detect deviations. Furthermore, the navigational data is interpreted in relation to the traffic, traffic rules, and voyage data. This data (e.g., anomaly detection, route monitoring) is shown on the Electronic Situation Picture Display.
- Level 3: Prediction of the ship course and the course of other vessels can be used to identify potential collisions and to warn the operator.

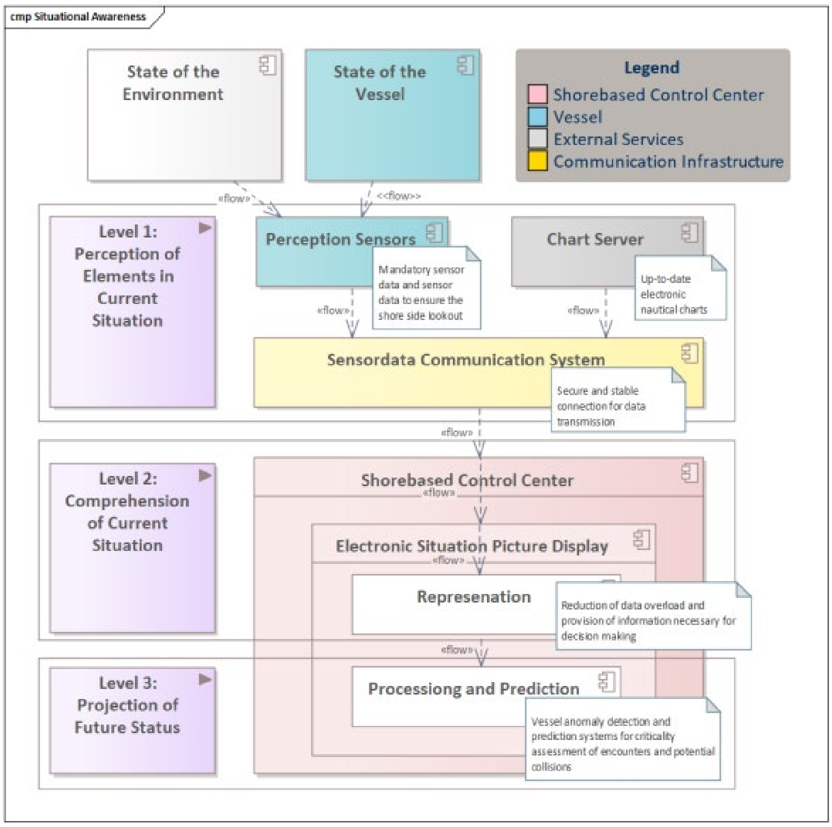


Figure 30: Generic ROC architecture from AVATAR , copied from Lamm, Piotrowski, Hahn (2022).

In addition to the components for situation awareness, the architecture includes a component for remote steering which can be connected to different external input devices like joysticks, azimuth levers, ship consoles, or touchpads.

In order to test the technical feasibility, the architecture was developed as a prototype (Figure 31) within the eMIR maritime testbed (see 7.4 below).

Figure 31: Prototype of a mobile ship bridge for a ROC, copied from Lamm (2022).

7.3 How have safety and security for ROCs been addressed?

At the time when the State-of-the-Art report was finished (March 2023), no specific information on safety or security analysis in the AVATAR project could be found.

7.4 Which legal aspects have been considered?

In order to test and demonstrate the autonomous ship, AVATAR uses the e-Maritime Integrated Reference Platform (eMIR) (Lamm 2022). eMIR (Rüssmeier, Lamm, Hahn 2019) supports the required research and development processes for automated system functions and technologies along the whole development process. With its comprehensive and integrated test bed, consisting of two components, eMIR enables the execution of simulations and physical experiments. The virtual part, HAGGIS, is based on a co-simulation infrastructure using High Level Architecture (HLA). LABSKAUS, the physical part, can then seamlessly access the HAGGIS elements. The overall test process therefore moves successively and as seamlessly as possible from virtual to physical tests.

The open testbed design of eMIR supports a system engineering approach through cooperation schemes and human-machine interfaces on which the overall system can be built. eMIR uses a common data model based on the international S-100 standard for maritime data exchange. The HAGGIS simulators are maintained in Oldenburg at the German Aerospace Institute for Systems Engineering (DLR-SE) and in Hamburg at the Federal Maritime and Hydrographic Agency (BSH). LABSKAUS covers the area of the River Elbe between Brunsbüttel and Cuxhaven, and the sea area between Cuxhaven, Wilhelmshaven, and Helgoland. Further physical test sites for autonomous shipping research are planned in cooperation with Jade-Weser-Port in Schillig, Reede, and to the west of Helgoland.

The ROC architecture was implemented as a prototype. This resulted in a mobile bridge system (Figure 31) with suitable communication infrastructure for communication with an automated ship. For field trials, the bridge system was integrated in a container to allow transportation of the system to different test locations (Figure 32).

Using eMIR, the technical feasibility of the architecture for the ROC was tested (Lamm, Piotrowski, Hahn 2022). This included testing the delays of the communication between ship and SCC. The tests confirmed the general technical feasibility.

Figure 32: Mobile ROC in form of a transportable container, copied from Lamm (2022).

7.5 Statements and Findings

For our study, the following statements and findings have been derived from the AVATAR project:

Nr.	Statement / Finding	Source	Category
SoA-AV-1	A system architecture that matches and supports the three levels of human situation awareness (as defined by Endsley) is suggested.	AVATAR	C2

SoA-AV-2	For performing tests in simulators and in the field, using the e-Maritime Integrated Reference Platform (eMIR) is suggested.	AVATAR	C4

8. LOAS (National Project, Norway)

Project name:	Land-based Operation of Autonomous Ships
Runtime:	2019 - 2023
Website:	https://prosjektbanken.forskningsradet.no/en/project/FORISS/296527?Kilde=FORISS&distribution=Ar&chart=bar&calcType=funding&Sprak=no&sortBy=date&sortOrder=desc&resultCount=30&offset=90&TemaEmne.1=Maritim
Consortium: Kongsberg Maritime (KM), Institute for Energy technology (IFE) and the Norwegian University of Science and Technology (Norges teknisk- naturvitenskapelige universitet -NTNU).	
Objective: “Develop and test interaction solutions for a Remote Operation Centre (ROC) that ensures safe and effective monitoring of one or more ships that are wholly or partly unmanned.” (Kaarstad, Braseth 2020).	

8.1 Which automation use cases are investigated?

Ship:	all-electric urban passenger ferry (milliAmpere2), length 8.5m, beam 3,5m, speed 3-5 kn
Level of automation:	Automated without crew on board
Route/Area:	Canal-crossing service over a 100m long urban canal in Trondheim

8.2 How is the ROC structured and organised?

NTNU provides a Shore Control Lab to test design options (Alsos et al. 2022) for monitoring and control of autonomous ships. The lab can be used for example to control the milliAmpere urban ferry. Controlled experiments can be performed with the real ferry but also with a simulated version of the ship in a simulated environment. The infrastructure supports these experiments with systems for recording the sensor data from the autonomous ship and for recording sound and videos of the operators and their interaction with the human-machine interface. Furthermore, biometric data can be recorded from the operators. The screens and interactive components can be configurated differently and it is possible to test new ideas for the human-machine interface.

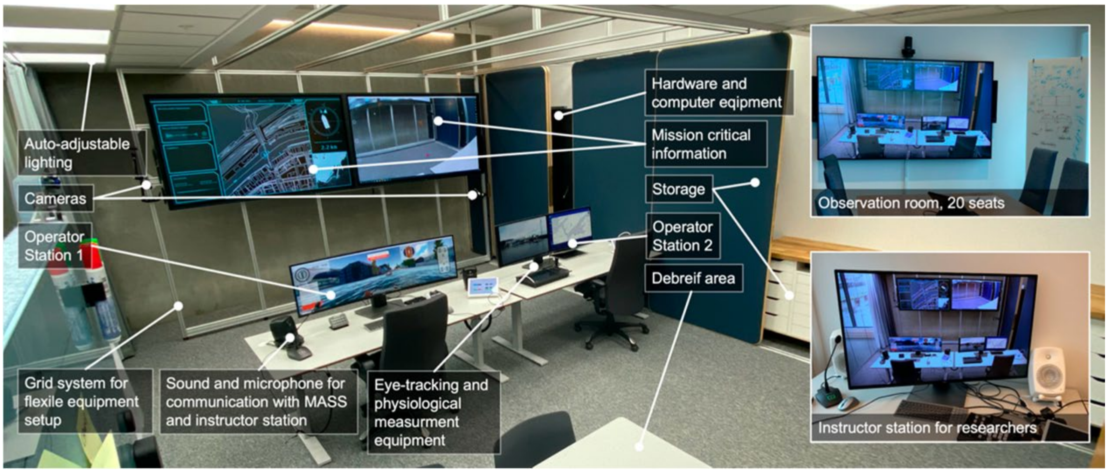


Figure 33: Structure of the NTSU Shore Control Lab, copied from Veitch and Alsos (2021).

Some of such new ideas have been described by Porathe (2021). He suggests using a digital twin of the ship, or of the autonomous decision-making system (the “expert system” as he calls it) in the ROC. In case of communication glitches involving the ship status, this digital twin can be used to simulate the ship behaviour, and in this way to extrapolate the situation in the future.

Furthermore, Porathe (2022) suggests a “Quickly Getting into the Loop Display” (QGILD). The QGLID (Figure 34) is designed for situations in which an operator is monitoring several ships and suddenly one of these ships reports an emergency that requires deeper investigation and a decision from the operator. Now they must get into the loop quickly.

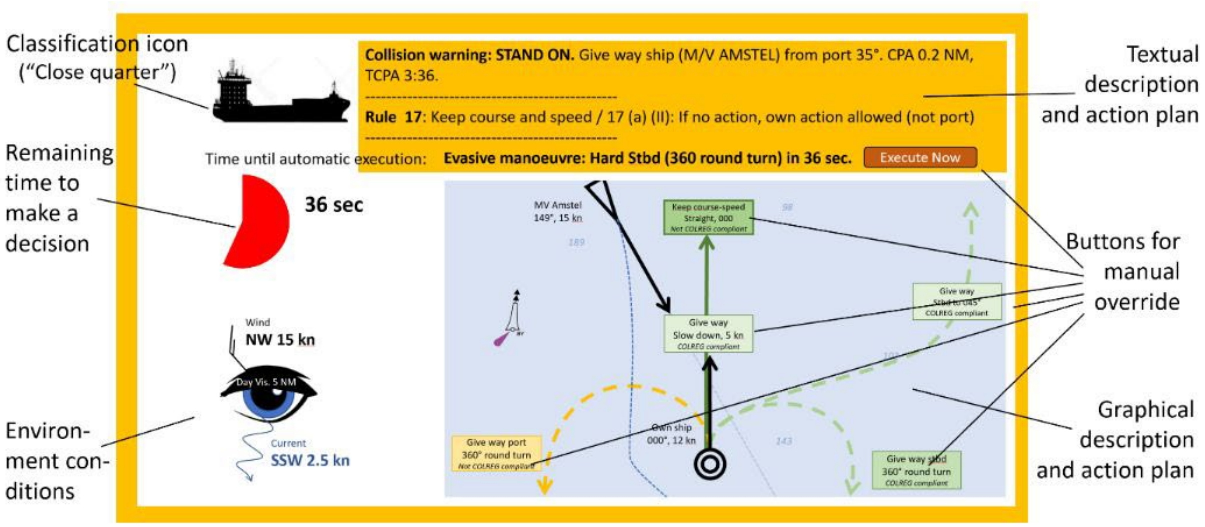


Figure 34: HMI of the QGILD, copied from Porathe (2022).

The QGLID includes the following three ingredients (Porathe 2021, 2022):

- Tactical update: The QGLID provides a comprehensive overview of the problem situation (Figure 34):
  - a classification item that shows the type of problem: “close quarters” (showing icon of ship type, size, and aspect), “mechanical failure”, or “navigation hazard”,
  - remaining time to make a decision,
  - environment conditions (e.g., wind, current), the eye glyph shows visibility status: daylight/good visibility, night-time/good visibility, daylight somewhat reduced visibility, and finally restricted visibility.
- Automation transparency: The automated system (the “expert system”) must communicate its understanding of the situation and its plan to solve the problem. Porathe (2021) stresses the point that the automation should always have a plan (a minimum risk manoeuvre as a last resort). In Figure 34, a textual description of the problem (“a give-way vessel approaching on the own ships port side”), the COLREG rule which normally applies in this situation the system (rule 17), and the manoeuvre suggested by the automated system (since the other ship shows no sign consistent with the rule, the system suggests an evasive manoeuvre) is given. The tactical problem description is supplemented with a graphical problem statement. Figure 35 shows different plans for collision avoidance computed by the automation. The solid green line depicts the manoeuvre which is preferred by the automation. Other options are shown as dashed lines. For each option, a “certainty index” is given.

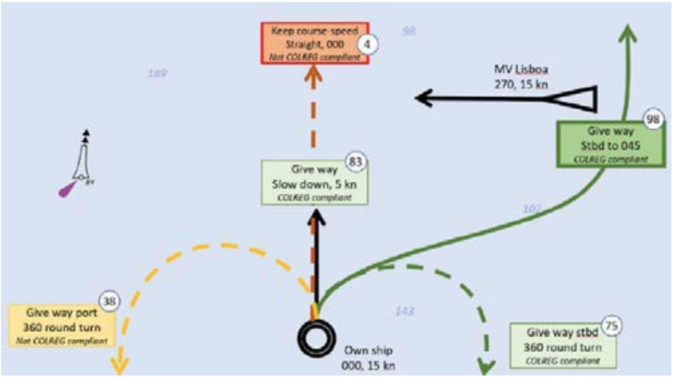


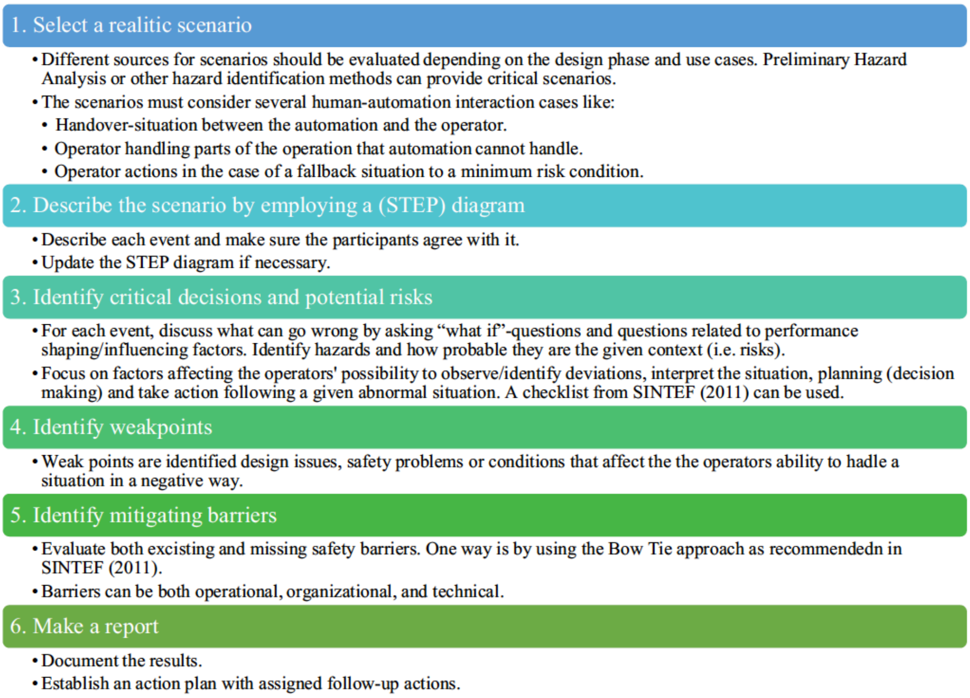
Figure 35: Automation transparency as provided by the QGILD, copied from Porathe (2021).

- Tools for intervention: The interface offers several buttons for interventions. The operator can for example, execute the evasive manoeuvre by clicking on the box “execute now” (Figure 34). Furthermore, they can choose between the different plans by clicking on one of the boxes which are associated with the different manoeuvre options. Additionally, the operator can take manual control and steer the ship by using a joystick.

8.3 How have safety and security for ROCs been addressed?

Hoem, Veitch, and Vasstein (2022) defined a method for analysing the risk involved in the interaction between human operators and automation. They called this method the Scenario Analysis Method. It is based on the Crisis Intervention and Operability study (CRIOP): “CRIOP is a methodology that contributes to verification and validation of the ability of a control centre to safely and efficiently handle all modes of operations, including start up, normal operations, maintenance and revision maintenance, process disturbances, safety critical situations, and shut down.” (Johnsen et al. 2008). CRIOP has intensively been applied to analyse offshore control centres of the Norwegian Oli & Gas industry. It “focuses on the interaction between people, technology and organisations” (Johnsen et al. 2008) and thus specifically addressed the human factor. CRIOP includes four steps: 1) Prepare & organise, 2) General Analysis, 3) Scenario Analysis, and 4) Implementation & Follow-up. The new method of Hoem, Veitch, and Vasstein uses step 3 as a starting point and extends the scenario analysis to include the analysis of hazards and risks, identification of weak points and derive design improvements. Figure 36 shows an overview of the six steps. The main part consists of discussing a set of critical scenarios in an interdisciplinary workshop with relevant subject matter experts. The scenarios are formalised in the form of STEP diagrams. The method shall be used as part of the design process of the ROC to guide design decisions concerning the human-machine interaction.

The new method has been evaluated using the hand over from automated to manual control in an ROC for the milliAmpere ferry as a case study.



1. Select a realitic scenario

- Different sources for scenarios should be evaluated depending on the design phase and use cases. Preliminary Hazard Analysis or other hazard identification methods can provide critical scenarios.
- The scenarios must consider several human-automation interaction cases like:
  - Handover-situation between the automation and the operator.
  - Operator handling parts of the operation that automation cannot handle.
  - Operator actions in the case of a fallback situation to a minimum risk condition.

2. Describe the scenario by employing a (STEP) diagram

- Describe each event and make sure the participants agree with it.
- Update the STEP diagram if necessary.

3. Identify critical decisions and potential risks

- For each event, discuss what can go wrong by asking “what if”-questions and questions related to performance shaping/influencing factors. Identify hazards and how probable they are the given context (i.e. risks).
- Focus on factors affecting the operators' possibility to observe/identify deviations, interpret the situation, planning (decision making) and take action following a given abnormal situation. A checklist from SINTEF (2011) can be used.

4. Identify weakpoints

- Weak points are identified design issues, safety problems or conditions that affect the the operators ability to hadle a situation in a negative way.

5. Identify mitigating barriers

- Evaluate both excisting and missing safety barriers. One way is by using the Bow Tie approach as recommendedn in SINTEF (2011).
- Barriers can be both operational, organizational, and technical.

6. Make a report

- Document the results.
- Establish an action plan with assigned follow-up actions.

Figure 36: Scenario analysis method, copied from Hoem, Veitch, and Vasstein (2022).

As a starting point of the evaluation a concept of operation (CONOPS) and a preliminary hazard analysis have been performed prior to the workshop. The handover of control to the SCC was identified as critical. A STEP diagram is prepared which shows the handover procedure step-by-step:

- milliAmere detects unexpected object (e.g., a partly submerged log) in the pathway and asks for assistance,

- milliAmpere stops and stays in position,
- milliAmpere send notification to ROC: attention needed,
- ROC operator recognizes notification and clicks on "assess",
- ROC operator investigates the object by switching camera angles,
- milliAmpere shows which sensor is not able to detect object,
- ROC operator decides on action: take manual control,
- ROC operator notifies passengers on action taken,
- ROC operator uses joystick to manoeuvre ferry around the object.

This representation of the scenario is discussed in the workshop by asking questions like "What can go wrong?", "What would the operator wish to do in each situation?", "How is the ROC operator notified?", "What information is presented?", "What happens if the information is not presented?", "How can the information be misunderstood?", and "Which erroneous decisions can be made?"

In this way, the experts identify hazards, the probability of the hazard, and potential barriers to avoid or mitigate the risk. For the milliAmpere use case, the following points were identified by Hoem, Veitch, and Vasstein (2022):

- "The existing CONOPS does not address the responsibilities of the SCCO. The role of the SCCO is a missing priority! A list of situations where immediate SC intervention is required must be established:
    - When and how should the operator intervene? Descriptions of tasks and supporting working procedures are needed.
- What are the needed skills and training for the SCCO?
- No alarm philosophy is established. Notifications on a screen alone are not enough.
- Recovering from a "safe state":
    - After going to a safe state and dropping the anchor, what happens?
    - What are the available resources to pick up passengers and resume operation? An emergency preparedness strategy is missing.
- Related to high-performance HMI: "easy to discover"-notification messages should appear centred on the main screen and not down in the left corner.
- Develop the GUI to support explainable artificial intelligence:
    - Bounding box around detected object to avoid misunderstanding which object is within the collision zone and detected by the ferry.
    - Implement layers showing the collision zone when necessary.
- A safety management system must be established: how can the SCCO report incidents (an unplanned, uncontrolled event that under different circumstances could have resulted in an accident), near-accidents (an event that could reasonably have been an accident but did not, typically due to the SCCO intervening), and accidents (an unintended sequence of events that lead to harm to people, environment, or other assets)?
- More data from actual experiments are needed, i.e. systematic recording of accidents and incidents in the testing phase.
- Maintenance issues: How will the SCC handle this? How is the status of the technical systems presented to the SCCO?"

The evaluation of the new method shows that risks could be identified which have not been uncovered with other risk analysis methods. But the authors have also listed issues that might limit the validity, credibility, and reliability of the method (Hoem, Veitch, Vasstein 2022):

- "Biases from the participants already involved in the HMI-design process,
- lack of having the actual end-user present,
- time constraints,
- limited opportunities to modify the ferry's design, configurations, and technical solutions."

8.4 Which legal aspects have been considered?

Within the LOAS project, a review of the maritime regulatory framework was performed to investigate how "operation of autonomous ships [is] incorporated into governing documents?" (Kaarstad, Braseth 2020). The authors investigated the following issues: jurisdictional concerns, regulations for safe manning - preventing collisions at sea, regulations for safe manning - obligation to assist persons in distress at sea, regulations for safe manning - the role and competence of remote operators, protection of the maritime environment, cyber security, and anti-terror protections. They concluded that:

- The lack of an IMO framework leads to rather different interpretations by the (flag) states of existing regulations with regard to autonomous ships.
- An update of existing regulatory instruments is needed.
- "Technical standards for sensor-based lookout functions, remote operation, and system-based decision-making are needed to be developed from scratch."
- "Generic requirements regarding redundancy, cybersecurity, certification, and training are also needed."

8.5 Statements and Findings

For our study, the following statements and findings have been derived from the LOAS project:

Nr.	Statement / Finding	Source	Category
SoA-LO-1	Using a digital twin of the ship is suggested in case of communication glitches involving the ship's status to simulate the ship's behaviour and in this way to extrapolate the situation in the future.	LOAS	C2
SoA-LO-2	A Quickly Getting into the Loop Display (QGILD) is suggested for situations in which an operator monitors several ships and suddenly needs to handle an emergency on one of them.	LOAS	C3
SoA-LO-3	Automated systems must communicate their understanding of the current situation and their plan to solve a prevailing problem.	LOAS	C2
SoA-Lo-4	The HMI should provide means to override the automation (tools for intervention).	LOAS	C3
SoA-LO-5	A method for risk assessment based on the Crisis Intervention and Operability study (CRIOP) is suggested.	LOAS	C4
SoA-LO-6	Technical standards for sensor-based lookout functions, remote operation, and system-based decision-making do not exist and need to be developed from scratch.	LOAS	C4
SoA-LO-7	Generic requirements regarding redundancy, cybersecurity, certification, and training are needed.	LOAS	C4

9. Seafar (Private Company, Belgium)

Project name:	Seafar Remote Navigation
Runtime:	Founded
Website:	https://seafar.eu
Consortium: Seafar cooperates with the Port of Antwerp and De Vlaamse waterweg (for approval). Further cooperation exists with the shipping companies Decloedt and Celis.	

Seafar plans a new remote-control center in Duisburg Germany MASS World (2022). Here they cooperate with HGK Shipping and Reederei Deymann.
Objective: “Seafar supports and operates automated vessels from a Shore Control Center.”[2]

9.1 Which automation use cases are investigated?

Ship:	12 vessels[3] ranging from 38m (400T) up to 110m (3000T)
Level of automation:	Remotely operated / full crew onboard (Antwerpen to Zeebrügge), Remotely operated / crew reduced (Antwerpen to Mastricht), Remotely operated / unmanned (Ostende to Diksmuide)[4].
Route/Area:	Inland routes from Diksmuide to Ostend, from Antwerpen to Zeebrügge, from Antwerpen to Mastricht

9.2 How is the ROC structured and organised?

Seafar provides a “proven design” (Bargsten, Schippers 2022) for remote control. The design foresees (Bargsten, Schippers 2022):

- “Control station + Traffic Control”
- “2 captain control rule / four eyes principle”
- “Traffic control support”

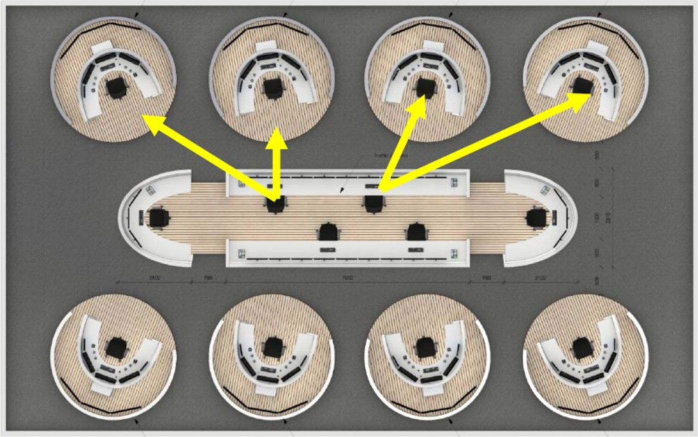


Figure 37: Control room design, copied from Bargsten and Schippers (2022)

From the pictures used by Seafar, it can be assumed that the video feeds from onboard cameras are in the centre of the control stations for remote-control. Figure 38 shows a 3D-model of the remote-control station. Pictures of the implemented control stations are available on the Seafar website[7]:

---

[2] https://seafar.eu
[3] https://smartmaritimenetwork.com/2022/02/22/unmanned-vessel-control-centre-opens-in-antwerp/
[4] https://unece.org/sites/default/files/2022-06/WP.15-AC.2-40-inf02e.pdf

Figure 38: Remote control station 3D model, copied from Bargsten and Schippers (2022)

9.3 How have safety and security for ROCs been addressed?

No public information on safety and security analysis methods could be found. But Pauwelyn and Turf (2023) point out that Seafar performs “a project change application, an updated risk analysis, gap analysis and ConOps” for every change in the autonomy level of their ships.

9.4 Which legal aspects have been considered?

For the approval of their ships and ROC, Seafar is in is in regular contact with the Vlaamse Waterweg (Pauwelyn, Turf 2023).

Seafar performed tests with their Watertruck vessels, which are self-propelled barges. They are “certified under Flemish regulations, in accordance with Article 24, second paragraph of EU Directive 2016/1629 with regard to exemptions for vessels that travel limited routes of local importance or in port areas.” (Pauwelyn, Turf 2023)

The approval was mainly based on trials in inland waters (Pauwelyn, Turf 2023):

- 2019 tests in the Westhoek on the Yzer and the Plassendale-Nieuwpoort canal with Watertruck X (CEMT class II – bulk): experimental agreement defined that a crew had to be on board while the ship was remotely controlled from a SCC. The boat master on board could intervene and had the ultimate responsibility.

The experimental agreement was subsequentially adapted:

- In 2020, test with no crew but a technical superintendent on board. A skipper in the ROC had the ultimate responsibility. The technical superintendent acted only according to the instruction of the skipper.
- 2021 test with no crew on board. Safety procedures for these tests have been defined and demonstrated during the tests with crew on board.

Since 2020, further tests have been performed with the inland vessel Tercofin II (CEMT class Va - dry bulk/container) in the Albert Canal between the Port of Antwerp and Liège with the aim of reducing the crew on board. During these tests, there was always a crew on board, but parts of the full crew were situated in the ROC.

10. FernBin (National Project, Germany)

Project name:	Remote controlled inland vessel
Runtime:	07/2020 – 12/2023
Website:	www.fernbin.de/en
Consortium: DST – Development Center for Ship Technology and Transport Systems e.V., ISMT - Institute for Ship Technology, Ocean Engineering and Transport Systems, University of Duisburg-Essen, Argonics GmbH, Rhenus PartnerShip GmbH & Co. KG, RWTH Aachen University, Ingenieurbüro Kauppert, in - innovative navigation GmbH, BAW - Federal Waterways Engineering and Research Institute, HGK Shipping (associated partner)	
Objective: Develop a remotely controlled ship based on an existing ship (the GMS Ernst Kramer) provided by HGK Shipping and a remote-control station on shore – the ROC.	

10.1 Which automation use cases are investigated?

Ship:	Dry cargo ship with a length of 105 m and a beam of 9.5 m (the GMS Ernst Kramer)
Level of automation:	Remotely controlled
Route/Area:	Travelling from the Main via the Rhine to the Netherlands

10.2 How is the ROC structured and organised?

The ROC is developed at the Versuchs-und-Leitungszentrum Autonome Binnenschiffe (VeLABi)[5] in Duisburg. From the ROC, the remote operator ("the skipper") can steer the ship. Figure 39 shows the layout of the ROC and the direct control workstation. The general layout of the ROC displays (incl. radar, chart, and AIS) is similar to that of a conventional ship. The conventional "view from the window" is provided by cameras. The project partners intend to investigate the following elements for the ROC[6]:

- The HMI shows constantly changing information permanently while information only relevant for monitoring is presented in the background or is even hidden during regular operation. All information can be shown on demand.
- Different predefined display configurations can be retrieved by the skipper when needed.
- Various acoustic, optical, and haptic techniques are tested to warn the skipper in emergency situations.
- Mixed Reality (MR) visualisations are investigated, for example partial colourisation of camera images or text overlays on ships.

Furthermore, an assistance system for the remote operator ("the skipper") is developed, which predicts and visualizes the space required to encounter other ships safely. It includes a formal description of tasks like recognition, planning, decision-making and action control (Bejaoui, Söffker 2022). This formalisation has been achieved by observing captains and modelling their behaviour using Situation Operator Modelling. The model serves as a reference model

---

[5] https://www.velabi.de, in German only
[6] https://www.fernbin.de/en/work-packages

and can be used for two purposes: 1) to plan actions automatically, and 2) to evaluate the plausibility of actions performed by the skipper.

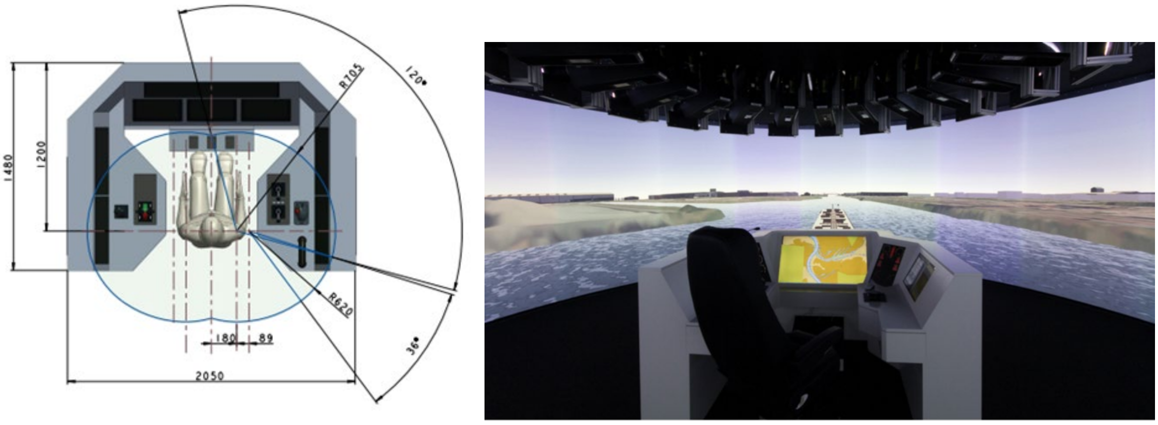


Figure 39: The layout of the ROC and direct control workstation in the FernBin project, copied from FernBin Website[7]

10.3 How have safety and security for ROCs been addressed?

Information about methods for safety and risk analysis could not be found, neither could information on security, at the time when the State-of-the-Art report was written. But the project plan of FernBin describes generic procedures for emergency situations[8].

Functionalities for detecting non-typical manoeuvres due to system errors, rule violations, system-internal errors, and other anomalies will be developed. If such anomalies are detected, the skipper will be warned. If the warnings are ignored, automation functions bring the ship into a safe and operational state. This will be achieved by steering the ship automatically out of the shipping channel and stopping the engine. If a collision cannot be avoided, an emergency stop is performed and associated emergency routines are started.

10.4 Which legal aspects have been considered?

Existing regulations like ES-Trin, the Inland Navigation Road Regulations, and the Rhine Navigation Passenger Regulations are analysed and suggestions for additions and changes are made[9].

To get acceptance for the remotely controlled ship, testing is first done in simulators step by step: testing of the data link in the entire test field, testing of direct control, testing of control with increasing use of assistance systems, and finally testing of failure scenarios. The final tests are performed in the field.

10.5 Statements and Findings

For our study, the following statements and findings have been derived from the FerBin project:

Nr.	Statement / Finding	Source	Category
SoA-FB-1	An assistance system to evaluate the plausibility of actions performed by a remote operator is suggested	FerBin	C2

---

[7] https://www.fernbin.de/en/projekte/wp-5200-ude.

[8] https://www.fernbin.de/en/work-packages/

[9] https://www.fernbin.de/en/work-packages/

11. DFFAS (National Project, Japan)

Project name:	Designing the Future of Full Autonomous Ship
Runtime:	2020 - 2022
Website:	https://www.nippon-foundation.or.jp/en/news/articles/2022/20220301-67775.html[10]
Consortium: Japan Marine Science Inc. (Project Leader); MTI Co., Ltd.; IKOUS Corporation; BEMAC Corporation; SKY Perfect JSAT Corporation; TOKYO KEIKI INC.; Nippon Telegraph and Telephone Corporation; NTT DOCOMO, INC., Japan Radio Co., Ltd.; NYK; FURUNO ELECTRIC CO., LTD.; Weathernews Inc.; EIZO Corporation; NTT Communications Corporation; Japan Hamworthy Co., Ltd.; Japan Marine United Corporation; Nabtesco Corporation; Nippon Shipping Co., Ltd.; pluszero Inc.; Honda Heavy Industries Co., Ltd.; Yokogawa Denshikiki Co., Ltd. and Mitsubishi Research Institute Inc.	
Objective: “aims to develop a crewless vessel with open collaboration. It also aims to develop autonomous navigation and support functions such as monitoring and diagnosis from shore (including a communication system) and remote operation in emergencies.” (Nakashima et al. 2022)	

11.1 Which automation use cases are investigated?

Ship:	Container ship “Suzaku”, 749 GRT
Level of automation:	Autonomous with maintenance crew in board
Route/Area:	Congested inland waters, round trip between Port of Tsu-Matsusaka and Port of Tokyo, 424 NM

11.2 How is the ROC structured and organised?

The ROC in DFFAS is a Fleet Operation Centre (FOC). Figure 40 shows the high-level organisation of the FOC, and the tasks and the communication with the MASS (Ando et al. 2022). In nominal situations, the ship is navigating autonomously. In off-nominal cases, the FOC takes over and operates the ship remotely. The ship performs a Minimal Risk Manoeuvre in an emergency. The operational status is computed by a System Status Manager component based on 1) waypoints, 2) the internal health level of the manoeuvring, propulsion, and communication subsystems, and 3) the environmental conditions in relation to the operational domain. This results in four operational statuses:

- Normal: Running without any involvement by the operator.
- Active monitoring: Running under monitoring and verification by the operator.
- Remote fallback: Running under fallback operations by the operator at FOC.
- Independent fallback: Running under fallback operations by the machinery on the vessel, to keep the system at Minimal Risk Condition

The dynamic sharing of responsibilities and distribution of roles between human and machine are defined for each status (Nakashima et al. 2022). Nakashima et al. (2022) foresee the following responsibilities:

- the shipowner is responsible for long-term voyage planning,
- strategic decisions are made on land,
- master and crew do the monitoring and perform fallback operations,
- the master acknowledges/approves changes in the operational status (e.g. from nominal to off-nominal),
- an oiler for the propulsion subsystem is on board for maintenance.

---

[10] Visited 22. Feb. 2023

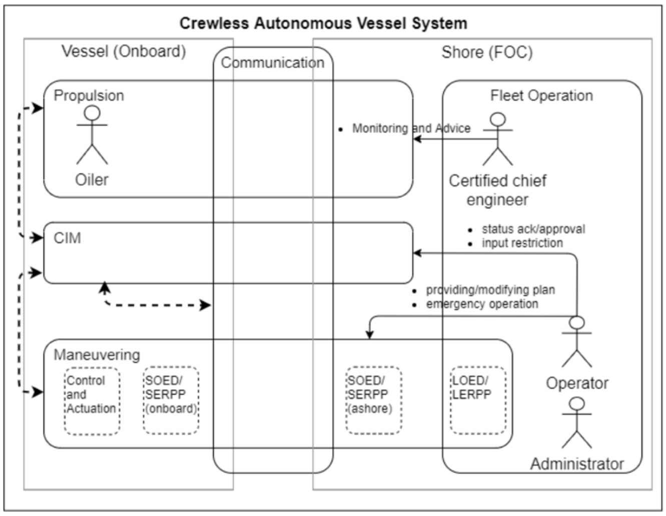


Figure 40: Use case diagram specification of the FOC organisation, tasks and communication with the MASS, copied from Ando et al. (2022)

Figure 41 shows the Integrated Display Block that is used for the following tasks:

- ship information collection,
- monitoring & analysis,
- engine remote monitoring,
- control & anomality detection.

Figure 41: Integrated Display Block in the FOC, copied from Ando et al. (2022).

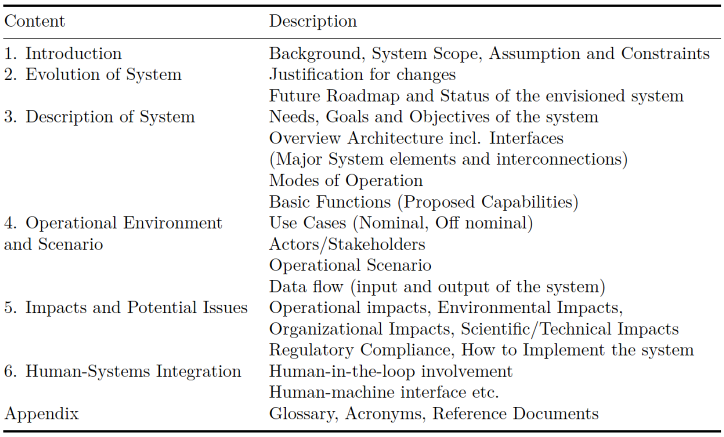
Figure 42 shows the Emergency Response Block that is used for remote control functions.

Figure 42: Emergency Response Block in the FOC, copied from Ando et al. (2022).

11.3 How have safety and security for ROCs been addressed?

Safety has been addressed by defining the Concept of Operations (ConOps) and by performing a System Theoretic Process Analysis (STPA).

The Concept of Operation (ConOps) was prepared by defining the users, associated usage scenarios, external environment, and other external constraints for the autonomous navigation system. Figure 43 shows the structure and contents of the ConOps document.

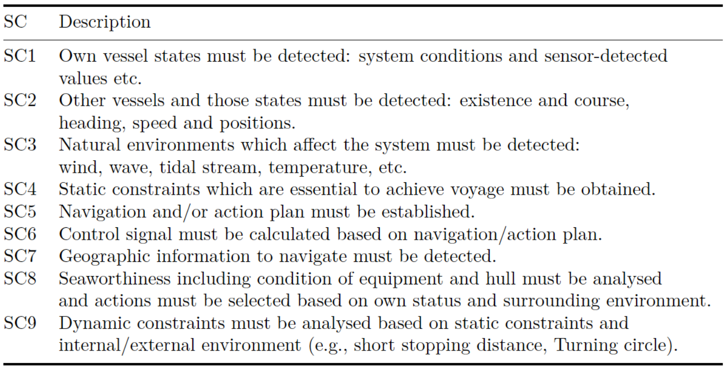


Content	Description
1. Introduction	Background, System Scope, Assumption and Constraints
2. Evolution of System	Justification for changes Future Roadmap and Status of the envisioned system
3. Description of System	Needs, Goals and Objectives of the system Overview Architecture incl. Interfaces (Major System elements and interconnections) Modes of Operation Basic Functions (Proposed Capabilities)
4. Operational Environment and Scenario	Use Cases (Nominal, Off nominal) Actors/Stakeholders Operational Scenario Data flow (input and output of the system)
5. Impacts and Potential Issues	Operational impacts, Environmental Impacts, Organizational Impacts, Scientific/Technical Impacts Regulatory Compliance, How to Implement the system
6. Human-Systems Integration	Human-in-the-loop involvement Human-machine interface etc.
Appendix	Glossary, Acronyms, Reference Documents

Figure 43: Concept of Operation (ConOps), copied from Nakashima et al. (2022).

The STPA performed in the project consist in four steps:

- Step 0-1: first, the accidents and hazards of the system are identified. From these, Safety Constraints (SCs) for the system are derived. The focus of the analysis is on collisions and groundings, with fire and other incidents excluded.



SC	Description
SC1	Own vessel states must be detected: system conditions and sensor-detected values etc.
SC2	Other vessels and those states must be detected: existence and course, heading, speed and positions.
SC3	Natural environments which affect the system must be detected: wind, wave, tidal stream, temperature, etc.
SC4	Static constraints which are essential to achieve voyage must be obtained.
SC5	Navigation and/or action plan must be established.
SC6	Control signal must be calculated based on navigation/action plan.
SC7	Geographic information to navigate must be detected.
SC8	Seaworthiness including condition of equipment and hull must be analysed and actions must be selected based on own status and surrounding environment.
SC9	Dynamic constraints must be analysed based on static constraints and internal/external environment (e.g., short stopping distance, Turning circle).

Figure 44: Safety constraints for the system, copied from Nakashima et al. (2022).

- Step 0-2: The control structure is defined. The structure defined in the project is the one shown above in Figure 40.
- Step 1: The interaction between subsystems in the control structure is analysed with regard to potential “unsafe control actions” (UCA), e.g., how might the interaction between CIM and Manoeuvring go wrong. To identify the UCAs, the following so-called guide words (e.g., not provided, too early, too late) have been applied:
  - a control action required for safety is not provided or is not followed,
  - an unsafe control action is provided that leads to a hazard

  - a potentially safe control action is provided too late, too early, or out of sequence
  - a safe control action is stopped too soon or applied for too long (for a continuous or non-discrete control action).
- Step 2: For each UCA, Hazard Contribution Factors (HCF) are identified. Furthermore, countermeasures for the HCFs are identified. These countermeasures are formulated as safety requirements and are inputted into a model-based design process where the safety requirements are assigned to system components and are iteratively refined along the iterative decomposition of the systems into subsystems.

In order to define cybersecurity measures, guidelines from three sources have been used as a reference (Nakashima et al. 2019):

- The Guidelines on Cyber Security Onboard Ships from BIMCO (Baltic and International Maritime Council) (BIMCO et al. 2018),
- The ABS Guide for Cybersecurity Implementation for the Marine and Offshore Industries from American Bureau of Shipping (2018),
- The Framework for Improving Critical Infrastructure Cybersecurity from the National Institute of Standards and Technology (NIST 2018).

The main cyber security measure is the isolation of execution and control functions from external networks.

11.4 Which legal aspects have been considered?

Within the DFFAS project, Bureau Veritas (2022) delivered an Approval in Principle (AIP) to NYK and its group companies MTI Co., Ltd. and Japan Maritime Science Inc. “for a fully autonomous ship framework that is currently being developed under the name of APExS-auto.” APExS-auto (Action Planning and Execution System for Full Autonomous) is a technological framework for the realisation of a crewed autonomous ship. It was used in DFFAS to develop the fully autonomous ship demonstration.

11.5 Statements and Findings

For our study, the following statements and findings have been derived from the XYZ project:

Nr.	Statement / Finding	Source	Category
SoA-DF-1	A responsibility scheme with five roles is suggested: ship owner, certified chief engineer, operator, administrator, oiler.	DFFAS	C1
SoA-DF-2	For safety analysis, a method based on System Theoretic Process Analysis (STPA) is suggested.	DFFAS	C4

12. Further Maritime Projects

12.1 Rolls-Royce

In 2016, Rolls-Royce (2016) released a video on YouTube showing their vision for a future ROC. The research for this concept was done by Rolls-Royce in cooperation with VTT Technical Research Centre of Finland and the University of Tampere’s research centre, Tampere Unit for Computer Human Interaction (TAUCHI).

The monitoring station shown in the video can be seen in Figure 45 (left). The big wall screen shows an overview of the traffic situation and the planned route of the monitored ship. In case of problems (e.g. communication with ship is lost), diagnostic information can be overlaid (Figure 45, right).

Figure 45: Monitoring station, copied from Rolls-Royce (2016).

For closer inspection, the operator can send drones to the ship which then transfer a live video feed (Figure 46). In this way, the operator might for example detect that an antenna is broken.

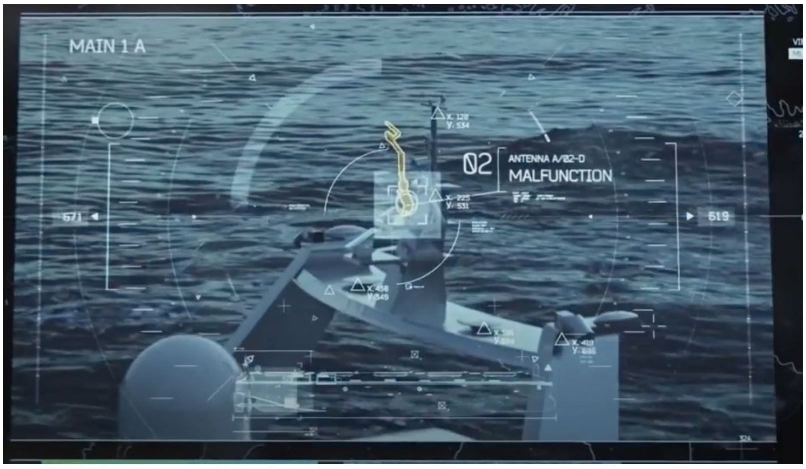


Figure 46: Video stream from drones, copied from Rolls-Royce (2016).

An engineer can use the wall screen to display more detailed diagnostic information (Figure 47, left) including sound recordings for example of an engine (Figure 47, right).

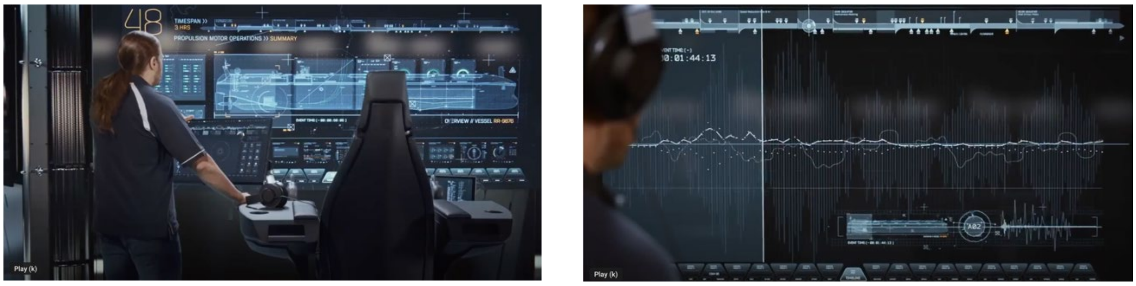


Figure 47: Detailed diagnostic information for error analysis, copied from Rolls-Royce (2016).

A collaboration table (Figure 48) supports “in-depth situation analysis and reviews”. Technical problems and resulting decisions can be discussed and planned in a team by referring to shared information.

Figure 48: Collaboration table, copied from Rolls-Royce (2016).

Tablets also play a role in the Rolls-Royce control centre. Some information (e.g. administrative documents) can be shown flexibly either on a wall screen or on a tablet (Figure 49, left). A tablet is also used to assign engineers to a ship in order to investigate a certain technical problem (Figure 49, right).

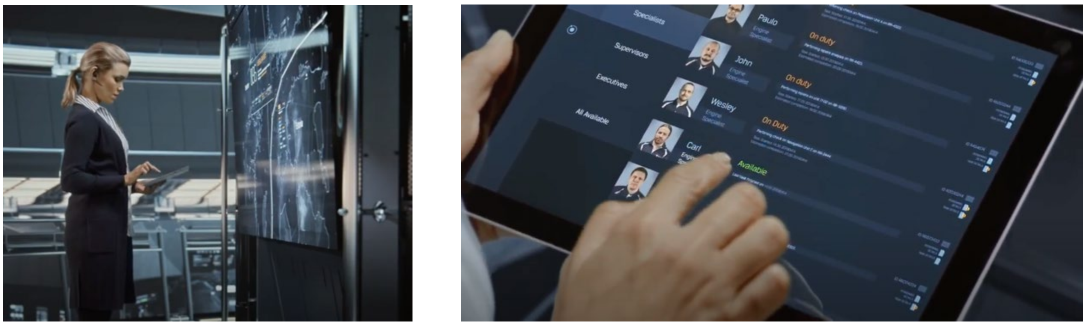


Figure 49: Use of tablets in the remote operating centre, copied from Rolls-Royce (2016).

In December 2018, Rolls-Royce and the ferry company Finferries demonstrated “the world’s first fully autonomous ferry” (Rolls-Royce 2018b). This demonstration was part of the project SVAN (Safer Vessel with Autonomous Navigation), a common project between Rolls-Royce and Finferries. The demonstrated ferry is called FALCO. It “is a 53.8 meter double-ended car ferry” and was operated in “the archipelago south of the city of Turku, Finland.” The ship was monitored from an ROC operated by Finferries. A captain could take control of the vessel in case of emergencies.

Nr.	Statement / Finding	Source	Category
SoA-RR-1	A design for an ROC is suggested.	Rolls-Royce	C1
SoA-RR-2	A wall screen layout is suggested, showing an overview of the traffic situation and the planned route of the monitored ship.	Rolls-Royce	C3
SoA-RR-3	Transfer of sound files from the engines is suggested for failure diagnosis.	Rolls-Royce	C3
SoA-RR-4	A collaboration table design is suggested to support “in-depth situation analysis and reviews” in case of failures.	Rolls-Royce	C3
SoA-RR-5	Ideas for using tablets in an ROC are suggested.	Rolls-Royce	C3

12.2 Kongsberg

In 2021, Kongsberg Maritime (2021) released a video on YouTube, which shows a futuristic concept for a Remote Operating Centre. Figure 50 shows the layout of this concept, which includes a Fleet Monitoring Station on an upper floor and Remote Operation Stations on a lower floor.

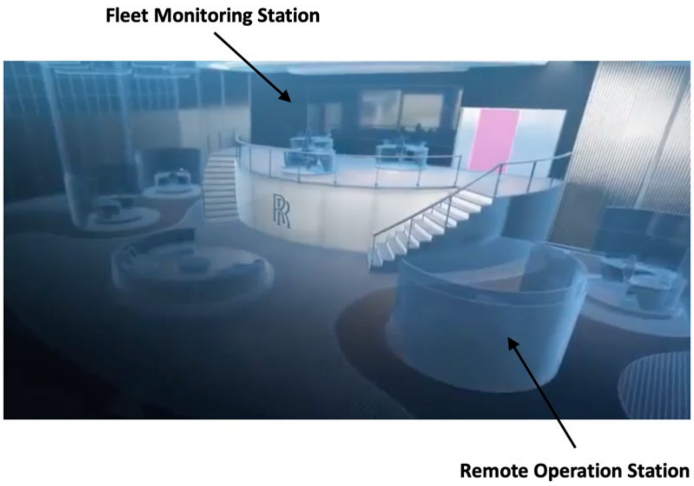


Figure 50: Layout of a Rolls-Royce Remote Operating Centre concept, copied from Kongsberg Maritime (2021).

The fleet management performs administrative routines and monitors all vessels of a fleet. At the Fleet Monitoring Station, an individual ship of the fleet can be selected, and the corresponding data can be analysed (Figure 51).

Figure 51: Fleet Monitoring Station, copied from Kongsberg Maritime (2021).

Fleet managers schedule and assign remote operation tasks to individual operators (Figure 52).

Figure 52: Assigning remote operation tasks, copied from Kongsberg Maritime (2021).

In critical situations, collaborative decision making and information sharing can be done at the Fleet Monitoring Station by referring to a wall screen that shows the traffic situation and planned routes (Figure 53).

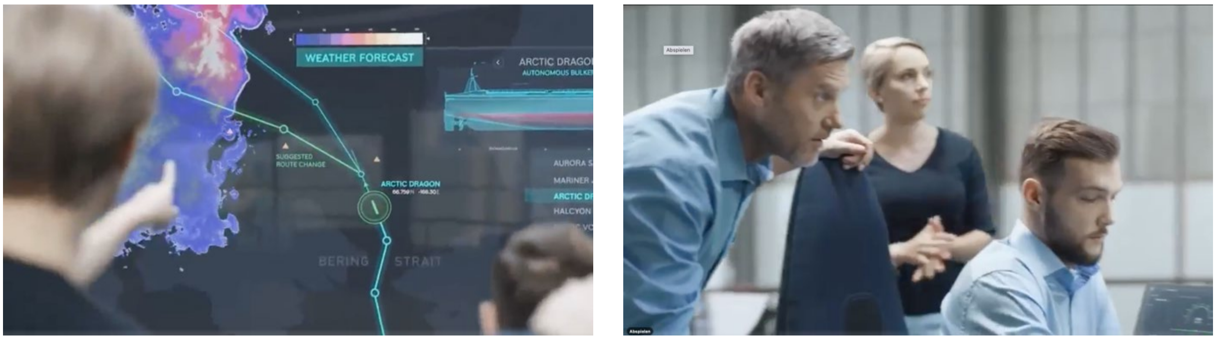


Figure 53: Collaborative decision making, copied from Kongsberg Maritime (2021).

At the Remote Operations Stations (Figure 54), the following task can be performed:

- check operation and status of critical vessel systems,
- communicate directly with port,
- remote control of the vessel e.g., during arrival into or departure from ports,
- activate autonomous control,
- adjust the vessel's route plan (Figure 55),
- hand the vessel back to the Fleet Monitoring Station.

Figure 54: Remote Operations Station, copied from Kongsberg Maritime (2021).

Figure 55: Adjusting the vessel's route plan, copied from Kongsberg Maritime (2021).

Via the Remote Operations Station, the centre can provide rest times to onboard crews by taking over watchkeeping duties (Figure 56).

Nr.	Statement / Finding	Source	Category

SoA-KG-1	A design for an ROC is suggested.	Kongsberg	C1
SoA-KG-2	A design for a Fleet Monitoring Station is suggested.	Kongsberg	C3
SoA-KG-3	A design for a Remote Operation Station is suggested.	Kongsberg	C3

Figure 56: Taking over watchkeeping duties from onboard crews, copied from Kongsberg Maritime (2021).

13. Further Projects from other Domains

In the following, we will present three projects from the Aviation domain and one project from the Rail domain which deal with remote control of automated vehicles.

13.1 INVIRCAT (Aviation, European Project, SESAR Joint Undertaking)

Project name:	Investigate IFR RPAS Control in Airports and TMA
Runtime:	07/2020 – 12/2022
Website:	www.invircat.eu
Consortium: DLR (Germany), CIRA (Italy), Deep Blue (Italy), EUROCONTROL (Europe), ISDEFE (Spain), ISSNOVA (Italy), NLR (Netherlands).	
Objective: “Create a concept of operations for remotely piloted aircraft systems in the terminal manoeuvring area of airports, assessing it through simulations and draft a set of recommendations for rule makers and standardization bodies.” (https://www.invircat.eu).	

13.1.1 Which automation use cases are investigated?

Vehicle:	Remotely piloted aircraft systems (RPAS)
Level of automation:	Remotely controlled aircraft equipped with an Automatic Take-Off and Landing (ATOL) system; no crew on board

Route/Area:	The project focusses on operation of RPAS in the Terminal Manoeuvring Area (TMA) airspace surrounding airports. All airports that are equipped with equipment for flight according to Instrument Flight Rules (IFR) are considered in general.

13.1.2 How is the ROC structured and organised?

The INVIRCAT project defines a generic concept of operation (ConOps) and derived requirements for the development and introduction of Remotely Piloted Aircraft Systems (RPAS) into the airspace and into the associated Standard Operating Procedures (SOPs). This includes concepts and requirements for the role of a Remote Pilot (RPIL) and an Air Traffic Control Operator (ATCO) as well as the cooperation between the two.

The RPAS are remotely controlled from a Remote Pilot Station (RPS). The RPIL is responsible for the operation of the RPAS at any time and shall always monitor the RPAS behaviour. The RPAS is assumed to be highly automated, but not autonomous. Just like traditional pilots, the RPIL communicates with the ATCO and adheres to the ATC clearance as well as to the pre-programmed flight plan. In the project, the tasks and responsibilities of the RPIL are defined according to four tasks groups (INVIRCAT Consortium 2021): Manage, Aviate, Navigate, and Communicate. Some of the tasks and responsibilities are the same as for traditional pilots while some are specific to RPILs (highlighted in bold, cf. INVIRCAT Consortium 2021:

- “Manage:
    - includes the overall planning, decision-making, and management responsibilities that must be accomplished by the pilot, supported by the HMI.
- Aviate:
    - Execute the flight according to the current flight plan.
    - Perform flight according to IFR.
    - Monitor and control aircraft systems, including automation.
    - Monitor consumable resources.
    - **Monitor and configure control station.**
    - **Monitor and control status of links.**
    - **Transfer control**.
    - Control and monitor location and flight path of the aircraft.
- Navigate:
    - Comply with clearances and instructions given by ATC.
    - Accept/reject ATC proposed alternative routings based on safety and feasibility.
    - Check NOTAM and other environmental information relevant to the flight.
    - Assume responsibility to remain inside/outside segregated areas according to the situation.
    - Assume responsibility to maintain own spacing from other aircraft when temporarily delegated by ATC.
    - Assume responsibility to maintain own spacing from terrain and obstacles on ground.
    - **Review and refresh lost link mission as necessary.**
    - **Terminate the flight, in the event such an action is deemed necessary, performing the termination procedure in the least harmful way to people or things as predictable**.
    - In general, stop the aircraft immediately if required for safety reasons or at the clearance limit during taxi operations.
- Communicate:
    - In order to perform its mission/operation, the RPIL is responsible for communication with ATC (or service providers).
    - Obtain information about present and forecasted weather for the pre-programmed flight plan.
    - Maintain a continuous listening watch on the appropriate ATC communications channels.
    - Request deviations of flight plan route if deemed necessary mainly for safety, operational, and/or economic reasons.
    - Obtain clearance from ATC prior to deviating from the cleared flight plan route.
    - When, for reasons of flight safety, deviation from the cleared flight plan route must be taken without clearance (e.g. following a TCAS advisory), inform ATC of actions taken as expeditiously as possible.
    - Obtain information on landing conditions from the destination airport’s information service (ATIS).
    - Provide ATC with mandatory information calls e.g., “on frequency, leaving frequency, leaving altitude, reaching altitude, start-up-request, taxi request, reaching assigned position” etc.
    - **In case of failure, perform appropriate Contingency Procedures, in particular**:

        - Contact ATC with any other available means.
        - In case of C2[11] link loss:
            - Contact ATC with any available means.
            - In case of degradation of Detect & Avoid capabilities, stop the RPAS and contact ATC with any available mean.
    - Communicate with other airspace users.
    - Communicate with crew members or ground support.“

For “Aviate” every RPAS shall be equipped with Automatic Take-Off and Landing (ATOL) system. This system gets input commands from a so-called Decision Maker. This function can either be taken over by the RPIL or by an RPAS module which supports the RPIL or takes decision in contingency situations.

Furthermore, the RPIL shall perform the flight-critical aviate-tasks without using visual aids, because this might lead to “pilot- induced oscillation (PIO) effects” due to latency in the video signal.

The introduction of RPAS in the Terminal Manoeuvring Area (TMA) is meant to have as little impact to current ATC operations as possible. But the operator must be aware of any RPAS in the area and must always be able to contact the RPIL. Furthermore, the ATCO must be “adequately trained in IFR ROPAS procedures.”

Apart from the RPIL and ATCO, further roles are defined (INVIRCAT Consortium 2021):

- RPAS Aircraft Operator: An organisation that carries out an aircraft operation. It has all the necessary skills and certificates. It is responsible for safety, missions, operational control, etc.
- Planner Controller: Coordinates sector traffic, and in Single Person Operations, handles planning and tactical aspects while assisting the Executive Controller. RPAS operations do not change the core responsibilities of the Planner Controller.
- Executive Controller: Manages air traffic and ensures flight safety within their Area of Responsibility. With RPAS operations, they also handle additional responsibilities such as coordinating with RPAS ground stations, providing instructions for safe separation, and overseeing procedures.
- Tower Runway Controller: Provides Air Traffic Services to aircraft in the control zone and near aerodromes. With RPAS introduction, they have added duties like coordinating with RPAS ground stations, applying higher separation values, and ensuring safety during failure.
- Ground Controller: Providing Air Traffic Service. For RPAS operations, the Tower Controller has added duties, including coordinating with RPAS ground stations, clearing the manoeuvring area, and maintaining safe separation during contingencies like C2 failure.
- Clearance Delivery Controller: Issues route clearances to aircraft before taxiing, including RPAS operations with added coordination responsibilities for RPAS ground stations and RPILs during certain phases.

The focus of the project is not on concrete designs for the remote control centre. But various setups for the Remote Pilot Station (RPS) have been used. These setups range from traditional cockpit setups (displays, side sticks, and throttle levers) to abstract designs in a control room setup. The concrete designs are not published in the project deliverables, but the setup used for validation of the ConOps is derived from the system architecture for RPAS defined in EUROCAE’s MASPS for RPS (EUROCAE 2020).

The HMI consists of three subsystems:

1. Critical C2 HMI: Components for these functions are expected to be avionics-grade equipment. The corresponding HMI consists of two segments:
    - Monitoring segment: Functions for monitoring aircraft data (position, attitude, air data), system status, and intended manoeuvres (flight trajectory, waypoints).
        - RPA health and state (latitude, longitude, altitude, airspeed, bank, pitch, yaw, engine settings, system health/warnings etc.)
        - Supports RPA/RPS handover and flight data recording.
    - Command and control segment: Functions, displays, and input elements for direct control over the control surfaces (aileron, elevator, and rudder), for the autopilot (setting of flight levels, airspeed, and waypoints), and feedback regarding the execution of the transmitted commands.
        - Makes it possible for the RPIL to modify the behaviour of the RPA (uplink)

---

[11] : C2 stands for control and command, meaning functions for flying and monitoring of RPAS.

        - Inputs to the RPA flight control system
        - Controls the settings of onboard avionics (transponder, ADS-B, etc.)
        - Supports RPA/RPS handover and flight data recording.

    The following function shall be available in the ATOL system in line with EUROCAE (2020):

    - Provide the RPIL with control to start and stop the execution of the automatic tasks.
    - Allow the RPIL to react to ATC instruction.
    - Allow the RPIL to manually activate and manage the execution of:
        - Contingency procedures
        - Holding procedure/resume approach
    - Provide the RPIL with situation awareness to:
        - Monitor the status of the ATOL.
        - Monitor the correct execution of the automatic task.
        - Detect ATOL occurrences.

2. Non-critical C2 HMI: Functions for specific mission functions or flight planning. Here, standard IT-equipment can be used.

3. Voice Intercom HMI: Functions for communication with the option to mute/unmute, or push-to-talk.
    - Enables voice/data communications between RPIL and ATC (and other pilots)
    - Voice may be relayed via the RPA or via other means.

INVIRCAT also considers requirements for the working position of the ATCO. The ATCO needs situational awareness of RPAS operations and thus for example, the following functions need to be provided (INVIRCAT Consortium 2021):

- "…highlight a change in the RPAS squawk code to 7400 to indicate a failure of the RPAS C2 link." 7400 is a squawk code for lost link.
- "Display the RPAS using a dedicated aircraft symbol or callsign."

13.1.3 How have safety and security for ROCs been addressed?

Security aspects are not considered in the project. With regard to safety, the INVIRCAT ConOps suggests an operational risk assessment in order to identify hazards, to evaluate risks, and to determine mitigations measures.

Figure 57 shows the steps involved in the operational risk assessment.

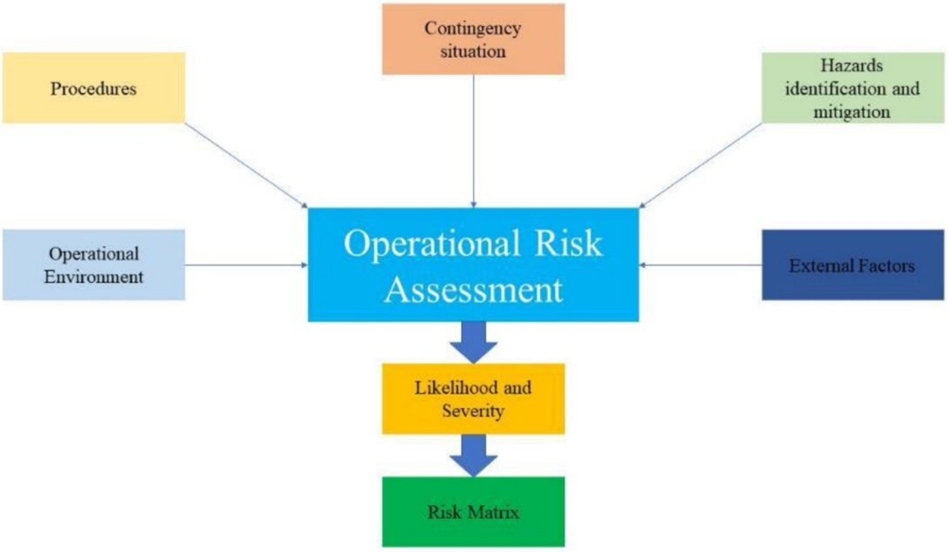


Figure 57: Operational risk, copied from INVIRCAT Consortium (2021).

- The operational environment (e.g., the airspace in the terminal area) is described in detail.
- Existing procedures (e.g., ATC, standard operational procedures) are described in detail.

- Contingency situations external to the concept and not under control, are identified: e.g., propulsion failure, partial propulsion failure, ATOL failure, C2 link failure, transponder failure, radio voice communication failure, missed approach, conflict, and fuel starvation.
- Hazards are identified.
- External factors are identified: e.g., bad weather conditions, bird strikes.
- The likelihood of hazards is assessed using the following terms:

Likelihood Class	Qualitative
Frequent (5)	Likely to occur many times (has occurred frequently)
Occasional (4)	Likely to occur sometimes (has occurred infrequently)
Remote (3)	Unlikely to occur, but possible (has occurred rarely)
Improbable (2)	Very unlikely to occur (not known to have occurred)
Extremely Improbable (1)	Almost inconceivable that the event will occur

- The severity of the hazards is assessed using the following categories:

Severity Category	Injuries	Safety	Crew workload
Catastrophic (A)	Aircraft or equipment destroyed / Multiple fatalities		
Hazardous (B)	Single fatality and/or Multiple serious injuries / Major equipment damage	Large decrease	Compromises safety
Major (C)	Non-serious injuries / Serious incident	Significant decrease	Significant increase
Minor (D)	None	Slight decrease	Slight increase
Negligible (E)	None	No effect	No effect

- By combining likelihood and severity, the risk is assessed using the three categories acceptable (green), tolerable (orange), or intolerable (red):

Safety Risk	Severity				
Probability	Catastrophic (A)	Hazardous (B)	Major (C)	Minor (D)	Negligible (E)
Frequent (5)	🟥 5A	🟥 5B	🟥 5C	🟧 5D	🟧 5E
Occasional (4)	🟥 4A	🟥 4B	🟧 4C	🟧 4D	🟧 4E
Remote (3)	🟥 3A	🟧 3B	🟧 3C	🟧 3D	🟩 3E
Improbable (2)	🟧 2A	🟧 2B	🟧 2C	🟩 2D	🟩 2E
Extremely improbable (1)	🟧 1A	🟩 1B	🟩 1C	🟩 1D	🟩 1E

Contingency procedures then have to be defined for the risks. In INVIRCAT, such procedures are described for example for the following risks:

- ATOL failure,
- C2 link failure,
- Voice communication failure,
- Missed approach.

13.1.4 Which legal aspects have been considered?

The ConOps is validated in several simulations (cf. INVIRCAT Consortium 2022a). A set of recommendations for rule makers and standardisation bodies is derived from the validated concept (INVIRCAT Consortium 2022b). This set includes requirements for the RPIL and the ATCO:

- "RPILs shall fly the RPAS following SOP as an on-board pilot would do at any moment and phase of the flight."
- "Standard operating procedures are applicable to RPILs when flying the RPAS."
- "The RPIL shall verify that all RPAS systems are fully functional during all phases of flight."
- "The RPIL shall verify that flight parameters are set correctly during all phases of flight."
- "The RPIL shall be aware of and declare contingencies to the responsible ATCO when there is a contingency situation."
- "ATCOs shall be aware of which aircraft is remotely piloted."

The INVIRCAT finally derives suggestions how to integrate the requirements into the current legal framework (cf. INVIRCAT Consortium 2022b).

13.1.5 Statements and Findings

Nr.	Statement / Finding	Source	Category
SoA-IC-1	The integration of autonomous vehicles into the existing traffic procedures must be clearly defined, e.g., Standard Operating Procedures (SOPs).	INVIRCAT	C1
SoA-IC-2	The status of the infrastructure should be monitored (lost links) by the remote operator.	INVIRCAT	C3
SoA-IC-3	Specific "lost links" and other contingency missions should be defined, which include informing traffic control.	INVIRCAT	C3
SoA-IC-4	Existing roles in traffic control must be able to identify autonomous vehicles and must follow specific procedures in some cases.	INVIRCAT	C3

13.2 DTT (Aviation, European Project, Horizon 2020)

Project name:	Digital Technologies for Tower
Runtime:	12/2019 – 03/2023
Website:	https://cordis.europa.eu/project/id/874470
Consortium: DLR (Germany), STICHTING KONINKLIJK NEDERLANDS LUCHT - EN RUIMTEVAARTCENTRUM (Netherlands), RIZENI LETOVEHO PROVOZU CESKE REPUBLIKY STATNI PODNIK (Czechia), LETOVE PREVADZKOVE SLUZBY SLOVENSKEJ REPUBLIKY, STATNY PODNIK (Slovakia), VALSTYBES IMONE ORO NAVIGACIJA (Lithuania), POLSKA AGENCJA ZEGLUGI POWIETRZNEJ (Poland), AUSTRO CONTROL OSTERREICHISCHE GESELLSCHAFT FUR ZIVILLUFTFAHRT	

MBH (Austria), HRVATSKA KONTROLA ZRACNE PLOVIDBE DOO (Croatia), UDARAS EITLIOCHTA NA HEIREANN THE IRISH AVIATION AUTHORITY (Ireland), LUFTFARTSVERKET (Sweden), NAVIAIR (Denmark), DFS DEUTSCHE FLUGSICHERUNG GMBH (Germany), ENAIRE (Spain), ENAV SPA (Italy), EUROCONTROL (Belgium), ATOS BELGIUM (Belgium), FREQUENTIS AG (Austria), HUNGAROCONTROL (Hungary), INDRA SISTEMAS SA (Spain), LEONARDO - SOCIETA PER AZIONI (Italy), AIRTEL ATN LIMITED (Ireland), SAAB AKTIEBOLAG (Sweden), SINTEF AS (Norway), AEROPORTS DE PARIS SA (France), AVINOR AS (Norway), HEATHROW AIRPORT LIMITED (United Kingdom), FLUGHAFEN MUNCHEN GMBH (Germany), SCHIPHOL NEDERLAND BV (Netherlands), SWEDAVIA AB (Sweden), FLUGHAFEN ZURICH AG (Switzerland), THALES LAS FRANCE SAS (France)
Objective: “to combine ATS [Air Traffic Services] services for several aerodromes from a Remote Tower Centre independent on airport location in order to make use of the valuable resource ATS provides more efficiently.” Additionally, the project investigated Virtual/Augmented Reality applications for tower and Automatic Speech Recognition (ASR) of Air Traffic Control utterances (DTT Consortium 2022). The analysis below focuses on the Remote Tower Centre organisation.

13.2.1 Which automation use cases are investigated?

Vehicle:	DTT does not deal with remote automated vehicles but with remote airports.
Level of automation:	Automation is not the focus of DTT but remote services for remote airports.
Route/Area:	From a remote tower centre, air traffic control services are provided to remote airports in rural areas.

13.2.2 How is the ROC structured and organised?

The project does not deal with the monitoring and controlling of automated vehicles, but with remote monitoring and controlling of airports. Control here means providing air traffic services like giving clearance, assigning runways, and the alike from a remote tower centre to pilots at the remote airport. In this way, air traffic controllers can provide such services to airports in rural areas without the need to be present at the site. DTT is interesting for this State-Of-The-Art study because it investigates a relevant organisation of the Remote Tower centre which might generate valuable insight for the organisation of an ROC.

DTT investigates among other topics how to balance workload between a group of air traffic controller operators (ATCO). This balancing is done by a remote tower centre supervisor (SUP). An ATCO needs to “keep a separate mental picture for each remote-controlled airport and safely switch between those.” (Friedrich, Timmermann, Jakobi 2022). This gets very challenging in high workload situations. Thus, workload balancing is crucial in this setting. Workload is induced by traffic volume and traffic mixture.

Figure 58 shows the organisation of a remote tower centre. The SUP supervises several Multiple Remote Tower Modules (MRTM) in the centre. A MRTM consists of one ATCO who controls three remote airports at the same time. The SUP communicates with the MRTM via voice or telephone. Information like weather and amount of traffic from the airports is transferred automatically. The MRTM provides an out-of-the-window view and/or radar for the different airports. The SUP has the following tasks:

- Main task:
    - gather pre-tactical data from all airports,
    - plan a distribution of airports onto MRTM,
    - implement this plan.
- Secondary tasks:

- to support each individual MRTM with additional coordination.

The goal of the SUP is to reduce the traffic load for each individual MRTM. This is done “with split & merge operations, which means the supervision of an airport is split from one MRTM and merged into another one.” (Friedrich, Timmermann, Jakobi 2022)

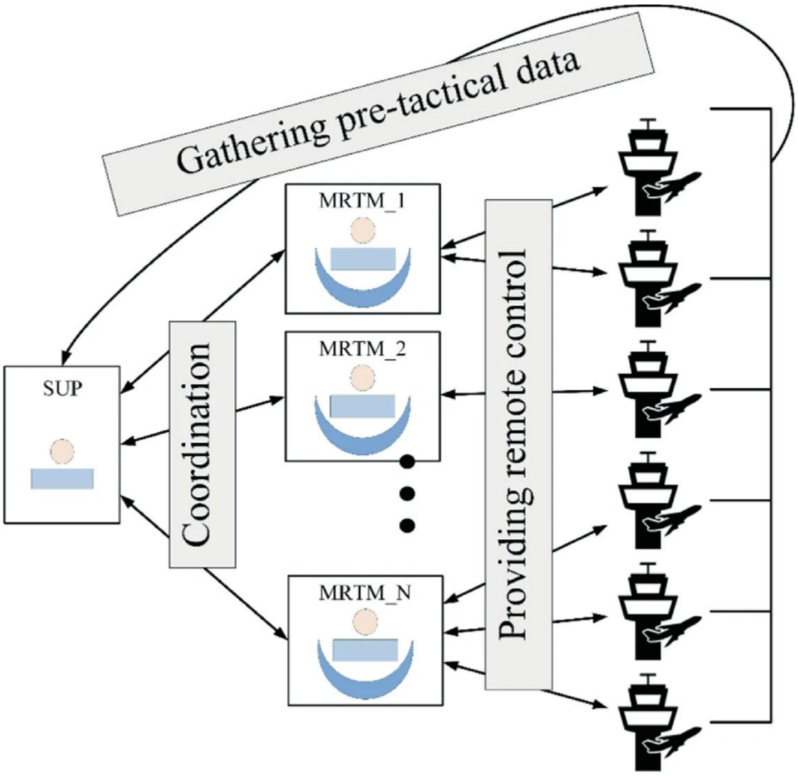


Figure 58: Concept of a remote-control room for Tower, copied from Friedrich, Timmermann, Jakobi (2022).

The SUP is supported by a tool. The functions of the SUP tool include (Friedrich, Timmermann, Jakobi 2022):

- An overview of airports assigned to the supervisor.
- Information on the opening and closing times of the airports.
- Weather and traffic density information as well as a technical overview of the airports.
- A pool of available ATCOs.
- The possibility to coordinate and merge airports and ATCOs via MRTM.
- Alerts for certain metrics such as excessive traffic.

13.2.3 How have safety and security for ROCs been addressed?

The organisation of the remote tower centre and the role of the SUP in particular was validated in a real time simulation study with 15 air traffic controllers (Friedrich, Timmermann, Jakobi 2021). The subjective handling and perceived safety were evaluated using questionnaires. The data analysis is based on descriptive data collected from these questionnaires.

The 15 participants were assigned to 5 groups of 3 participants. The setup for the study involved a workplace for a SUP and three MRTMs of which two were controlled by the participants and the third was a virtual workplace (Figure 59). This means that in each scenario, the SUP had to supervise three MRTMs. Each MRTM controlled up to three airports in parallel.

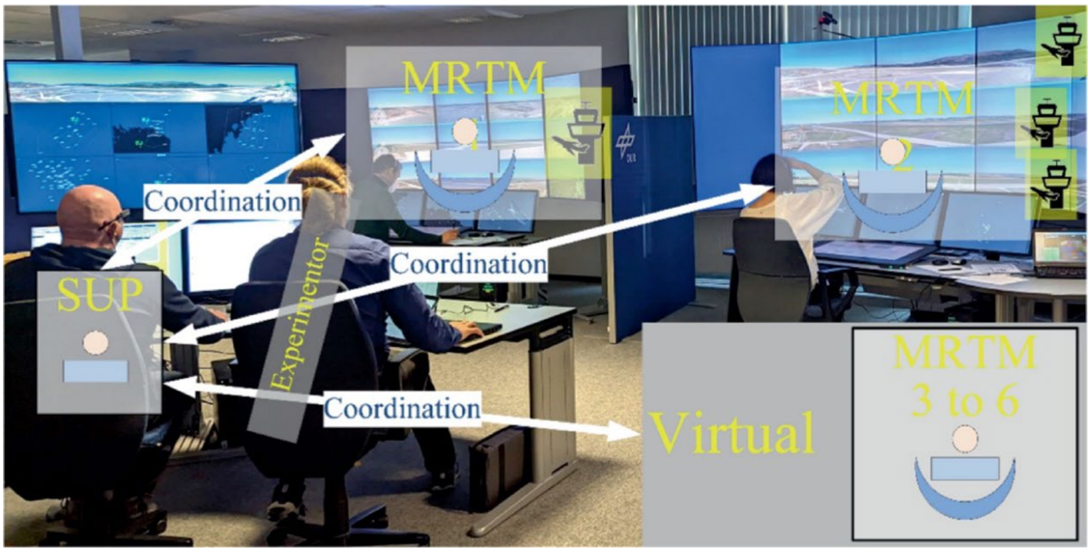
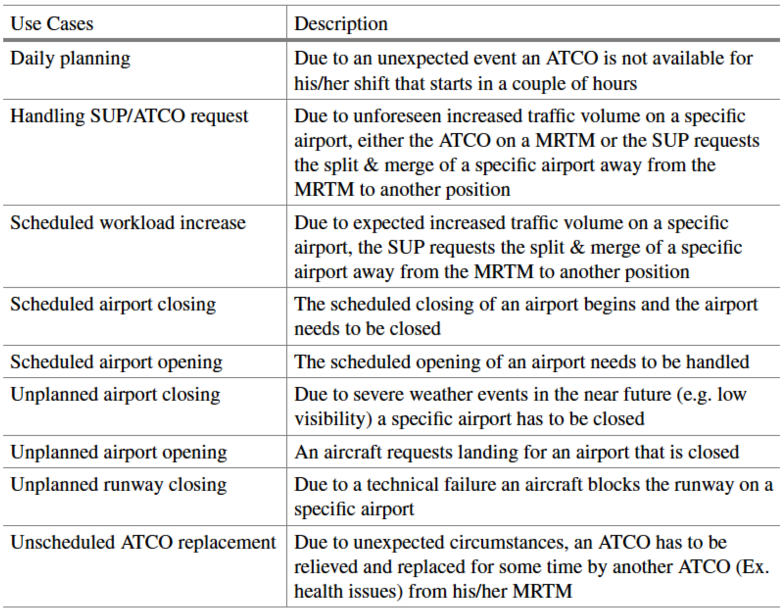


Figure 59: Organisation of the remote tower centre for the evaluation study, copied from Friedrich, Timmermann, Jakobi (2022).

Two scenarios were designed for the study. The participants of a group were randomly assigned to either SUP, MRTM 1, or MRTM 2. Each scenario was repeated three times resulting in six runs per group. The positions were changed after each run. During the scenarios, a number of use cases were triggered. These use cases are shown in Figure 60.



Use Cases	Description
Daily planning	Due to an unexpected event an ATCO is not available for his/her shift that starts in a couple of hours
Handling SUP/ATCO request	Due to unforeseen increased traffic volume on a specific airport, either the ATCO on a MRTM or the SUP requests the split & merge of a specific airport away from the MRTM to another position
Scheduled workload increase	Due to expected increased traffic volume on a specific airport, the SUP requests the split & merge of a specific airport away from the MRTM to another position
Scheduled airport closing	The scheduled closing of an airport begins and the airport needs to be closed
Scheduled airport opening	The scheduled opening of an airport needs to be handled
Unplanned airport closing	Due to severe weather events in the near future (e.g. low visibility) a specific airport has to be closed
Unplanned airport opening	An aircraft requests landing for an airport that is closed
Unplanned runway closing	Due to a technical failure an aircraft blocks the runway on a specific airport
Unscheduled ATCO replacement	Due to unexpected circumstances, an ATCO has to be relieved and replaced for some time by another ATCO (Ex. health issues) from his/her MRTM

Figure 60: Use cases for the real-time simulation study, copied from Friedrich, Timmermann, Jakobi (2022).

Using questionnaires, three aspects were evaluated:

- Was the use case controllable?
- Was situational awareness impaired?
- Did safety critical situations arise?

These are some of the study results:

- “general approval about the workplace itself”,
- “the SUP tool should provide needed information at the best time.”
- “the SUP tool was not as supportive as expected.”

- "the procedures were not defined clearly enough."

In general, the SUP workplace was perceived as positive. But some results raise "the idea to redefine the SUP even more as a supporter than a supervisor."

13.2.4 Which legal aspects have been considered?

Efforts were made in the DTT project to enhance regulations and guidelines (DTT Consortium 2022). The safety of multiple remote tower controls was addressed. In addition, a basis was created to promote the development of remote tower systems. This had already an impact on the EASA Guidance Material on remote aerodrome air traffic services. Another standard document is in preparation. Future updates could reduce restrictions and improve risk management measures.

13.2.5 Statements and Findings

Nr.	Statement / Finding	Source	Category
SoA-DTT-1	The role of a supervisor who distributes responsibilities for automated vehicles (remote towers) according to an assessment of the workload of remote operator should be considered.	DTT	C1
SoA-DTT-2	Workload assessment of remote operators should take into account traffic volume and traffic mixture.	DTT	C3

13.3 CORUS (Aviation, European Project, Horizon 2020)

Project name:	Concept of Operations for EuRopean UTM Systems
Runtime:	09/2017 – 11/2019
Website:	https://cordis.europa.eu/project/id/763551/results
Consortium: EUROCONTROL (Coordinator, Belgium), DFS (Deutsche Flugsicherung, Germany), DLR (Germany), DSNA (Direction des Services de la navigation aérienne, France), ENAV (Italy), HEMAV Technology (Spain), NATS (UK), UNIFLY (Belgium), Polytechnic University of Catalonia (Spain).	
Objective: "develop a reference Concept of Operations (CONOPS) for UTM (UAS [Unmanned Aircraft Systems] Traffic Management) in VLL [Very Low Level] airspace in Europe. … CORUS will develop an operational concept enabling safe interaction between all airspace users in VLL considering contingencies and societal issues."	

13.3.1 Which automation use cases are investigated?

Vehicle:	Unmanned aircraft (drones, small drones in particular).
Level of automation:	Unmanned drones, remotely controlled via drone pilot.
Route/Area:	Very low-level airspace in controlled (e.g., around airports) or uncontrolled areas.

13.3.2 How is the ROC structured and organised?

Aviation is highly regulated. In the DTT project, like in the INVIRCAT project, a major challenge is to integrate autonomous vehicles into the existing regulated environment by defining new rules which support safety and are consistent to the existing ones. The structure and organisation of an ROC in Aviation is highly connected to the rules and procedures of the airspace.

In CORUS, a ConOps for the operation of small drones in very low airspace has been defined and requirements for the design of vehicle functions, airspace services, and remote control have been derived. While the ROC itself hasn't been specifically designed, the CORUS ConOps makes it evident that the construction of an ROC should thoroughly consider the structure and procedures of the operating environment for remotely controlled or autonomous vehicles.

CORUS defines a ConOps for U-Space. U-Space is defined in the U-Space Blueprint by the SESAR Joint Undertaking (2017):

> “U-space is a set of new services and specific procedures designed to support safe, efficient and secure access to airspace for large numbers of drones. These services rely on a high level of digitalisation and automation of functions, whether they are on board the drone itself, or are part of the ground-based environment. U-space provides an enabling framework to support routine drone operations, as well as a clear and effective interface to manned aviation, ATM/ANS service providers and authorities. U-space is therefore not to be considered as a defined volume of airspace, which is segregated and designated for the sole use of drones. U-space is capable of ensuring the smooth operation of drones in all operating environments, and in all types of airspace (in particular but not limited to very low-level airspace). It addresses the needs to support all types of missions and may concern all drone users and categories of drones.”

The ConOps defined in CORUS regulates how drones can be operated in a U-Space environment. The following description of CORUS focusses on those aspects that are most relevant for an ROC. This includes the structure of the airspace, the roles involved in U-Space and drone operation, and the tasks/procedures to be performed before, during, and after a drone flight.

Structure of the airspace

The CORUS ConOps takes into account the structure of the drone airspace as it is defined in European regulations. In general, the drone airspace is organised accounting for 1) the services provided by the infrastructure, 2) the characteristics of the drone operations, and 3) the characteristics of the environment.

With regard to the services provided by the infrastructure, U-Space will be rolled-out progressively in four phases with increasing levels of services (U1 – U4, SESAR Joint Undertaking 2017, cf. Figure 61):

- **“U1: U-space foundation services** provide e-registration, e-identification, and geofencing.
- **U2: U-space initial services** support the management of drone operations and may include flight planning, flight approval, tracking, airspace dynamic information, and procedural interfaces with air traffic control.
- **U3: U-space advanced services** support more complex operations in dense areas and may include capacity management and assistance for conflict detection. Indeed, the availability of automated ‘detect and avoid’ (DAA) functionalities, in addition to more reliable means of communication, will lead to a significant increase of operations in all environments.
- **U4: U-space full services**, particularly services offering integrated interfaces with manned aviation, support the full operational capability of U-space and will rely on very high level of automation, connectivity and digitalisation for both the drone and the U-space system.”

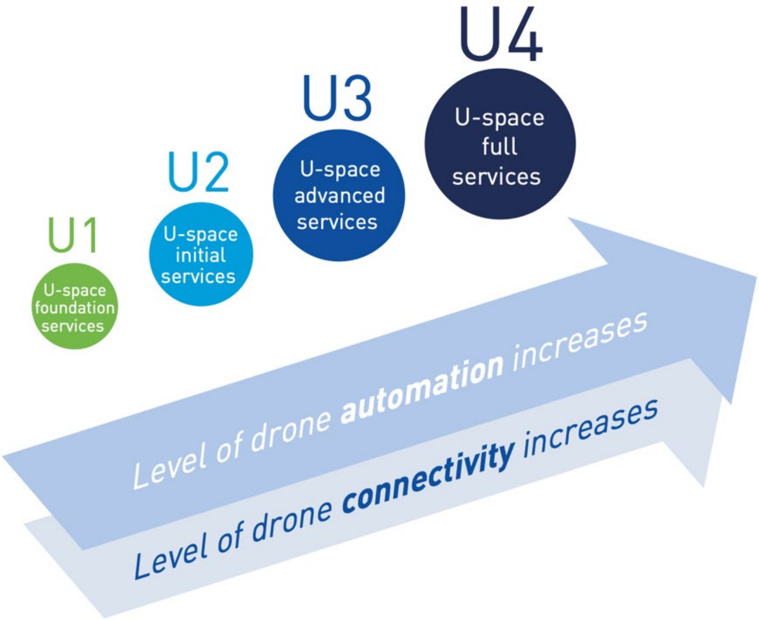


Figure 61: U-Space levels, copied from SESAR Joint Undertaking (2017).

The subsequent deployment of these levels depends on the availability of technology for drone automation and for interaction with the environment including manned and unmanned aircraft.

With regard to the characteristics of the drone operations, the European Union drone regulations categorise drone operations as open, specific, and certified (European Union 2019a). This categorisation is done based on a risk assessment (cf. Section 13.3.3). The following description of these categories just gives a rough definition and is not complete (cf. German Federal Ministry of Digital and Transport 2023):

- Open:
    - Applies when the drone weighs less than 25 kg, is not operated over assemblies of people, is operated at a maximum of 120 m above ground level, is operated in visual line of sight (VLOS) at all times, and does not carry persons or dangerous goods.
    - Drone operator does not have to be trained and experienced.
    - The drone does not have to be able to submit a position report.
    - A limited “follow-me” operation is necessary.
- Specific:
    - Applies when the drone weighs more than 25 kg, is operated at an above ground level of more than 120 m or in specific airspaces, or is operated beyond visual line of sight.
    - A Standard Scenario published by EASA has to be followed.
    - A Specific Operational Risk Assessment (SORA) has to be performed for the operation. The SORA must be described in an Operational Declaration. This declaration is quite generic and may cover many flights.
    - The drone operator needs a Light UAS operators Certificate (LUC).
    - The operation has to be performed in the framework of a flying club with appropriate authorisation.
- Certified:
    - Applied when the drone is operated over assemblies of people, dangerous goods are carried, or persons are carried.
    - The operation has to be EASE certified in compliance with all aviation norms and standards.
    - A type certificate is needed for the drone.

With regard to the characteristics of the environment, the following features are considered by the CORUS ConOps (Barrado 2020):

- “The numbers of drone flights that are expected;

- The ground risk—whether the area is populated;
- The air risk—the number of other flights in the volume, either manned or unmanned;
- Nuisance, security, or other public acceptance factors;
- The U-space services that are needed to enable safe operation."

The CORUS ConOps now takes into account the characteristics of the services, the characteristics of the drone operations, and the characteristics of the environment, and defines a structure of the airspace based on existing regulations from the European Commission on unmanned aircraft.

Firstly, the ConOps refers to flights in very low-level (VLL) airspaces. In CORUS, VLL is defined as (CORUS Consortium 2019a):

(1) "over the congested areas of cities, towns or settlements or over an open-air assembly of persons at a height less than 300 m (1 000 ft) above the highest obstacle within a radius of 600 m from the aircraft;"
(2) "elsewhere than as specified in (1), at a height less than 150 m (500 ft) above the ground or water, or 150 m (500 ft) above the highest obstacle within a radius of 150 m (500 ft) from the aircraft."

In addition to drone, this airspace is used by general aviation (GA): helicopters, military exercises, gliders and paragliders, etc. The ConOps "describes how VLL airspace should be organised and what rules and regulations should be put in place to enable the safe integration of drones with other users of this airspace, and what U-space services should be available to help the drone user achieve this."

VLL is divided into three different types of volumes: X, Y and Z, that differ mainly with regard to the provision of conflict resolution services (cf. Figure 62, CORUS Consortium 2019a):

- "X offers no separation services, all responsibility for safe operation is with the remote pilot."
- "Y offers strategic (= pre-flight) conflict resolution and usually traffic information during flight."
- "Z offers strategic conflict resolution and tactical (= in flight) conflict resolution"

In order to access Y and Z volumes an approved operational plan as well as appropriate training, technical equipment and a connected remote piloting station are needed.

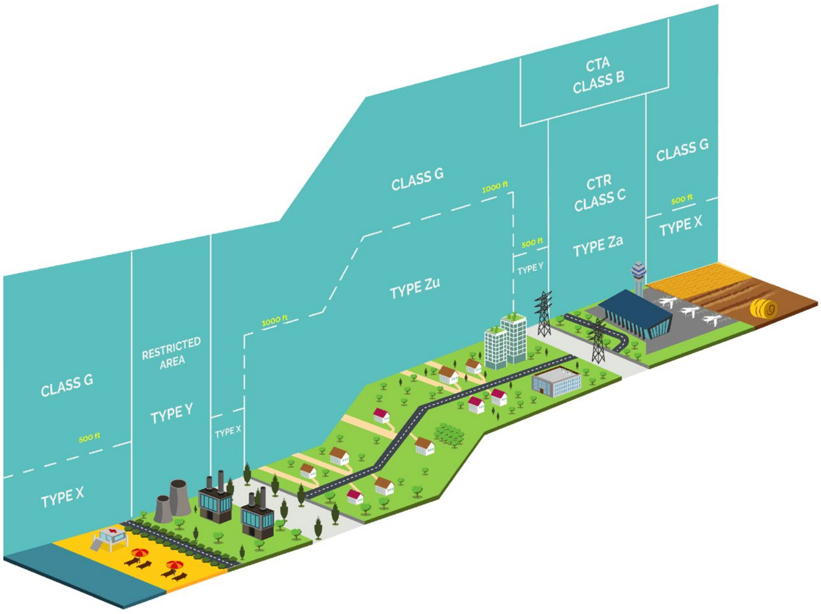


Figure 62: Airspace volumes for drones in Very Low Level airspace, copied from CORUS Consortium (2019a).

The ConOps defines which services are needed for which airspace volumes. Not all of these services are mandated for all volumes, some of them are recommended or even optional. The following list provides some examples of such services. It is not complete (cf. CORUS Consortium 2019b):

- Registration: “Interaction with the registrar to enable the registrations of the drone, its owner, its operator, and its pilot. Different classes of user may query data, or maintain or cancel their own data according to defined permissions.” Mandated in X,Y and Z volumes.
- Geo-awareness: “This provides geo-fence and other flight restriction information to drone pilots and operators for their consultation up to the moment of take-off. It includes existing aeronautical information, such as: restricted areas, danger areas, CTRs etc.; information extracted from NOTAMS, and legislation; temporary restrictions from the national airspace authority to produce an overall picture of where drones may operate.” Mandated in X, Y, and Z volumes.
- Geo-fence provision (incl. dynamic geo-fencing): “An enhancement of geo-awareness that allows geo-fence changes to be sent to drones immediately. The drone must have the ability to request, receive and use geo-fencing data.” Mandated in Y (where available), X and Z volumes.
- Operation plan processing: A safety-critical, access-controlled service that manages live operation plans submitted via the operation plan preparation service and checks them against other services. The service manages authorisation workflows with relevant authorities, and dynamically takes airspace changes into account. Optional for X, mandated in Y and Z volumes.
- Strategic Conflict Resolution: Checks for possible conflicts in a specific operation plan, and proposes solutions during operational plan processing. Not required for X, mandated in Y and Z volumes.
- Emergency Management: Provides assistance to a drone pilot experiencing an emergency with their drone and communicates emerging information to interested parties. Optional for X (where available), mandated in Y (where available) and Z volumes.
- Monitoring: Provides monitoring alerts (preferably audible) about the progress of a flight (e.g., conformance monitoring, weather compliance monitoring, ground risk compliance monitoring, electromagnetic monitoring). Optional in X, mandated in Y (where available) and Z volumes.
- Traffic Information: Provides the drone pilot or operator with information about other flights that may be of interest to the drone pilot; generally where there could be some risk of collision with the pilot’s own aircraft. Optional in X, mandated in Y and offered in Z volumes.
- Navigation Infrastructure Monitoring: Provides status information about navigation infrastructure during operations. This service should give warnings about loss of navigation accuracy. Optional in X and Y, mandated (where available) in Z volumes.
- Communication Infrastructure Monitoring: Provides status information about communication infrastructure during operations. The service should give warnings about degradation of communication infrastructure. Optional in X and Y, mandated (where available) in Z volumes.
- Collaborative Interface with ATC: “Offers verbal or textual communication between the remote pilot and ATC when a drone is in a controlled area. This service replaces previous ad-hoc solutions and enables flights to receive instructions and clearances in a standard and efficient manner.” Optional in X (when needed), mandated in Y (when needed) and Z volumes.

Roles

The ConOps also defines a set of roles differentiating between roles that provide or consume services (operational stakeholders), and others who just use information or data (non-operational stakeholders) from U-SPACE (Figure 63). In this State-of-the-Art Report, we will focus on the roles that consume services because they are the most important from an ROC perspective (CORUS Consortium 2019b):

- Drone Owner: “the legal entity, which can be a natural person, owning the drone. May be different from the Drone Operator legal entity (e.g., leasing rental mechanisms).”
- Drone Operator: “the legal entity, which can be a natural person, accountable for all the drone operations it performs. The equivalent of the airline for the pilot in manned aviation.”

Data and information are gathered from relevant stakeholders and then provided for example for drone operations. Using the services, the drone operator or drone pilot receives and provides the following information:

- Receiving:
    - Geo-fencing
    - Authorization
    - Constraints
    - Conflict alerts (warnings)
    - Traffic information for drone

  - Clearance/instructions
- Providing:
  - Identification
  - Positioning
  - Mission/Flight Intent
  - Drone Reporting
  - Accident/Incident Report

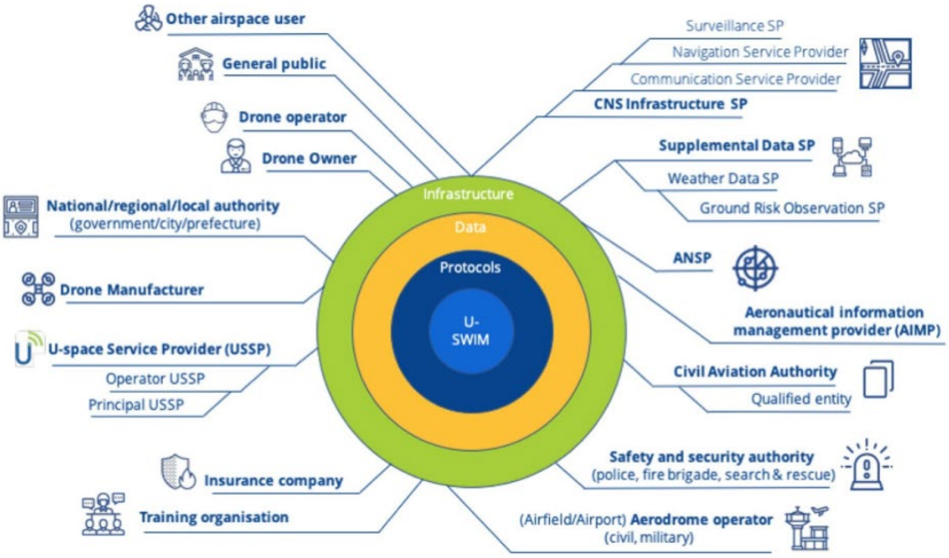


Figure 63: The U-Space stakeholders, copied from Barrado et al. (2020).

Tasks

The ConOps describes the tasks involved in a typical drone operation sequence. The dependence of the tasks on the structure and procedures of the regulated environment becomes highly evident. The ConOps differentiates between pre-flight, in-flight, and post-flight tasks (CORUS Consortium 2019a). Tasks that are connected to the regulated environment have been highlighted in italic:

- Pre-flight: divided in strategic and tactical tasks
  - Strategic:
    - *Registration of the drone if required*
    - *Registration of the drone operator*
    - *Pilot training (if applicable)*
    - *Registration of any pilot training*
    - *Procuring relevant insurance if not per-flight*
    - *Signing up with a U-space service provider*
  - Tactical:
    - *Becoming familiar with the location where the mission will occur as well as all environment services*
    - *(if appropriate) Selecting the appropriate drone and pilot to meet any airspace requirements*
    - *(if appropriate) Deciding on the type of operation; open, specific, certified*
    - *Planning the operation, which includes:*
      - *checking and planning appropriately for the airspace structure*
      - *checking whether any geo-fence crossing permission is required*
    - *(if appropriate) Performing SORA*
    - *(if appropriate) Submitting the Operation Plan, which results in:*

            - *Granting of any geo-fence crossing permit requested (in the form of a 'token' or electronic key)*
            - *Flagging any geo-fences that cannot be crossed*
            - *Strategic conflict resolution*
            - *(if appropriate) dynamic capacity management*
            - *Acceptance or refusal of the operational plan*
        - *Downloading the plan into the drone and/or remote piloting station (as appropriate)*
- In-flight:
    - *Prepare the flight area (if appropriate), including take-off and landing points*
    - *Verify the conditions for flight are within the limits planned: weather, airspace (geo-fences), other air traffic*
    - *Check the flight area for unexpected risks (such as the presence of people)*
    - *Check the Operation Plan (if any) is still OK*
    - *If not done previously, download the plan into the drone and/or remote piloting station (as appropriate)*
    - Prepare the drone for flight, check if it is airworthy and ready to operate, follow pre-flight checklist
    - Prepare the payload
    - *Log on to U-space and configure the Emergency Management Service for the current operation*
    - *Log on to the Position report submission sub-service send Start of Flight, enable position report submission (if used)*
    - Take-off
    - Fly, during which continuously monitor:
        - The drone's flight
        - The mission goal
        - Conformance with the plan
        - *Geo-awareness*
        - Other traffic – maintaining separation at all times
        - *Ground risk (people in particular)*
        - *Warnings from the Emergency Management Service*
        - *Traffic information if available*
        - *Tactical conflict resolution if available*
        - *Collaborative interface with ATC if available*
        - *Comms and Navigation infrastructure failure warnings if available*
    - Land
    - *Switch off position report submission, send End-of-flight (as appropriate)*
    - Go through end-of-flight checklist, e.g., power-off
    - *Log-off U-space*
- Post-flight:
    - Fill in a log or flight report as the operator's processes require
    - Check the mission has been successful
    - Check the drone
    - Either prepare for another flight or pack up

13.3.3 How have safety and security for ROCs been addressed?

CORUS defines a methodology for safety assessment as integral part of the ConOps: Methodology for U-space safety assessment (MEDUSA, CORUS Consortium 2019c). MEDUSA focuses on identification and mitigation of drone operations supported by U-Space services. It combines two perspectives: the perspective of the overall airspace system with its risks, and the perspective of single-missions with their risks. With regard to the airspace system, it considers 1) the airspace design, 2) the ATS service provision, and 3) the available U-Space services.

Figure 64 shows a high-level overview of the MEDUSA process:

- Success approach:
    - Pre-existing risks from unmanned aviation are used as a starting point to assess the effectiveness of the U-Space services in case they work as expected. Result: Requirements and specification of needed U-space services “in a given operational environment when considering all potential simultaneous or non-simultaneous drone operations.” (CORUS Consortium 2019c)
    - Next, abnormal conditions are considered. These are caused by external events which might have an impact on drone operations. Result: Additional requirements/mitigations allocated to drone operators or to organisations providing U-Space services.
- Failure approach
    - System-generated risks of the U-Space service are assessed in case U-space service provision fails. Considered are failures of systems and of procedures. Result: Integrity/reliability requirements and/or mitigations.

13.3.4 Which legal aspects have been considered?

In 2017 the SESAR Joint Undertaking (2017) published a Blueprint with a first concept for U-Space as a basis for safe and secure drone operations. The CORUS ConOps stared from this definition. Furthermore, CORUS considers Europeans Regulation on the classification of drone operations and the requirements for those operations (European Union 2019a, b). The results of the project can be the basis for extending the regulative framework for drone operations. A precondition for such regulative work is the validation of the ConOps, which was not the objective of the CORUS project.

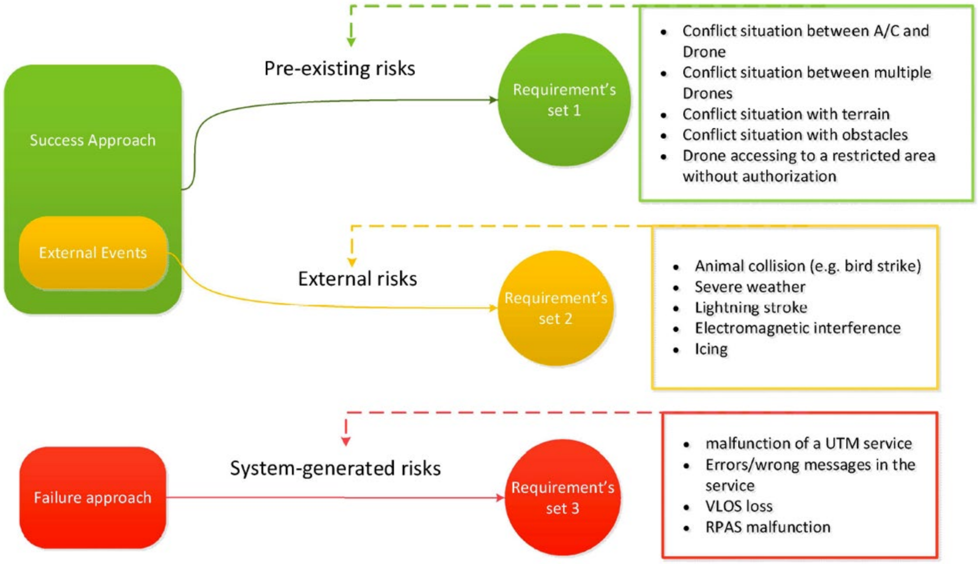


Figure 64: Methodology for U-space safety assessment (MEDUSA), copied fom CORUS Consortium (2019c).

13.3.5 Statements and Findings

Nr.	Statement / Finding	Source	Category
SoA-CO-1	The environment could offer specific services (e.g., registration, geo-awareness, conflict resolution, emergency management) to support safe, efficient, and secure access to the traffic space.	CORUS	C2
SoA-CO-2	The requirements for the operation of automated vehicles should be defined based on characteristics of	CORUS	C4

	the vehicle, its mission (incl. any risks), and its operational environment (incl. available services).		
SoA-CO-3	Safety analysis should take failures in the services provided by the environment into account	CORUS	C4

13.4 ARTE (Rail, National Project, Germany)

Project name:	Automated driven Regional Trains in Lower Saxony
Runtime:	2022 - 2025
Website:	https://www.static.tu.berlin/fileadmin/www/10002264/aktuelles/2022/010_017_Slimani_neu.pdf
Consortium: Alstom Transport Germany, German Aerospace Centre, Technical University Berlin	
Objective: The project investigates and demonstrates technologies for automated trains including obstacle and signal detection, re-location, and remote control. Additionally, changes in the operation of the trains including redistribution of the tasks and allocation of new tasks (e.g., in case of automation failures) are investigated and evaluated from a human factors' perspective. (Specht et al. 2022).	

13.4.1 Which automation use cases are investigated?

Vehicle:	Two Lint 41 trains will be equipped by ALSTOM Transport Germany with the European Train Control System (ETCS) as a technical basis for the Automatic Train Operation (ATO) application. These trains will be able to be operated autonomously.
Level of automation:	Autonomous with train attendant onboard (Grade of Automation 3) Autonomous without humans onboard (Grade of Automation 4)
Route/Area:	Train tracks in Lower Saxony, Germany

13.4.2 How is the ROC structured and organised?

The ARTE project researches, among others, three fields that are relevant for this State-Of-The-Art report (Specht et al. 2022):

- Changes in operation, technology, and roles: Changes that are induced by the automation of the trains in comparison to today's operation service are investigated. Based on these changes, requirements for people and technology are derived. Furthermore, job descriptions, needed qualification, and corresponding training for driverless operation are defined.
- Remote control operation: The role of the train attendant and the train operator as well as their synergies and needed human-machine interaction are investigated.
- Human factors: requirements for user-friendly, simplified remote control will be defined and tested.

Levels of increased automation in the rail domain are defined in the form of four Grades of Automation (GoA, Collart-Dutilleul, Levomte, Romanovsky 2019). In GoA 1 and 2, the train driver is still onboard. ARTE focusses on GoA 3 and 4, where the train is able to drive autonomously:

- GoA 3: train driver is not onboard (driverless train operation), train attendant is onboard, passengers are onboard.
- GoA 4: neither train attendant nor train driver are onboard (unattended train operation), also no passengers onboard.

In the rail domain, the human is seen as fall-back level entity who intervenes in case of failure of the automated system. ARTE defines fall-back tasks for the train attendant and train driver on GoA 3 and GoA 4 (Adebar, Milius, Naumann 2023). Figure 65 shows tasks that could be performed by the train attendant:

- Train attendant performs services for passengers (Figure 65-A): While taking care of the passengers, the train attendant could be informed about the status of the train and track via a tablet. Some minor problems might be solved by her/him directly via the tablet.
- Train attendant at the head of the train (Figure 65-B): In a separate room at the head of the train the train attendant could for example drive the train manually in case of failure.
- Train attendant performs physical work (Figure 65-C): In case of physical failures, the train attendant could perform minor repair work.

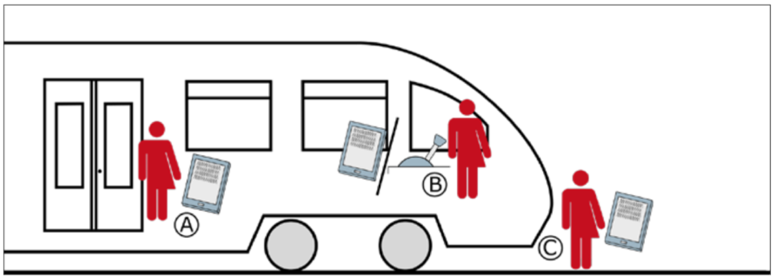


Figure 65: Work environment of the train attendant when acting as fallback level entity, copied from Adebar, Milius, and Naumann (2023).

Figure 66 shows task that could be performed by the train operator:

- Remote Operator, temporary monitoring (Figure 66-E): The remote operator is situated close to the tracks e.g., at a station. They could support by providing knowledge about the local track and the area. Furthermore, they could take direct control of the train via a tablet. This must be enabled via a video stream of the track.
- Remote Operator, continuous monitoring (Figure 66-F): The remote operator could be situated in a remote control centre and perform continuous monitoring of a number of trains. They take direct remote control of one train when a failure occurs.
- The train attendant (Figure 66-A) may support the remote operator.

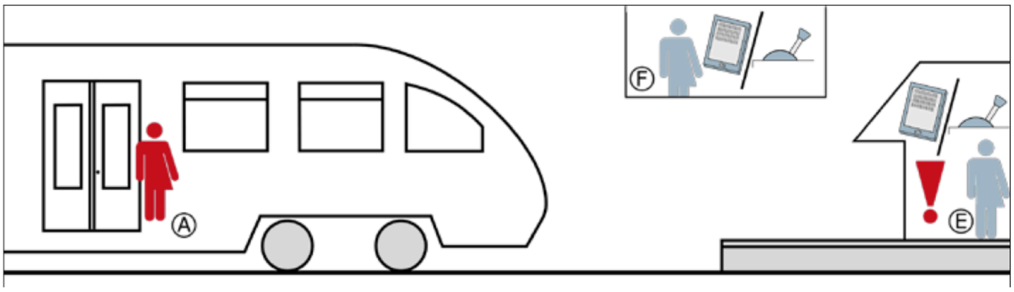


Figure 66: Work environment of the remote operator when acting as fallback level entity, copied from Adebar, Milius, and Naumann (2023).

Figure 67 shows potential synergies between train attendant and train operator:

- The remote operator (Figure 67-E-F) can check failure messages and initiate first actions to solve the problem without the need to interrupt the regular duties of the train attendant (Figure 67-A).
- The train attendant can support the remote operator by providing direct information on the situation or by performing tasks or assessments directly at the train (Figure 67-C).
- The train attendant can support visual monitoring of the track (Figure 67-A) when the remote operator assumes direct remote control of the train.

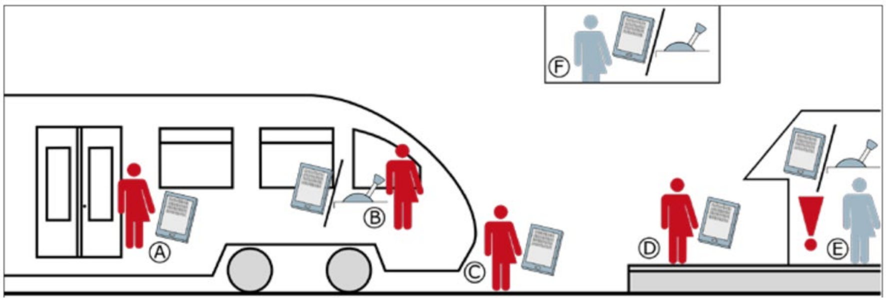


Figure 67: Synergies between train attendant and remote operator in fallback situations, copied from Adebar, Milius, and Naumann (2023).

The tasks of the train attendant and train operator in fall-back situations will be investigated and evaluated in the ARTE project from a human factors' perspective. At the time the State-Of-The-Art report was finalised, these results were not yet available.

Furthermore, the human-machine interaction will be designed in ARTE. A workplace designed by DLR (Brandenburger, Naumann 2018) will be used as a basis for the design of the ROC. This design is shown in Figure 68. The room is equipped with several workstations for remote monitoring and remote control performed by remote operator or so-called train operators (TO). Additionally, a shared knowledge space is mounted at the wall. It shows the positions and relevant operational information to all the remote operators. A specific workstation is foreseen for a signaller, who is responsible for the given area of operation.

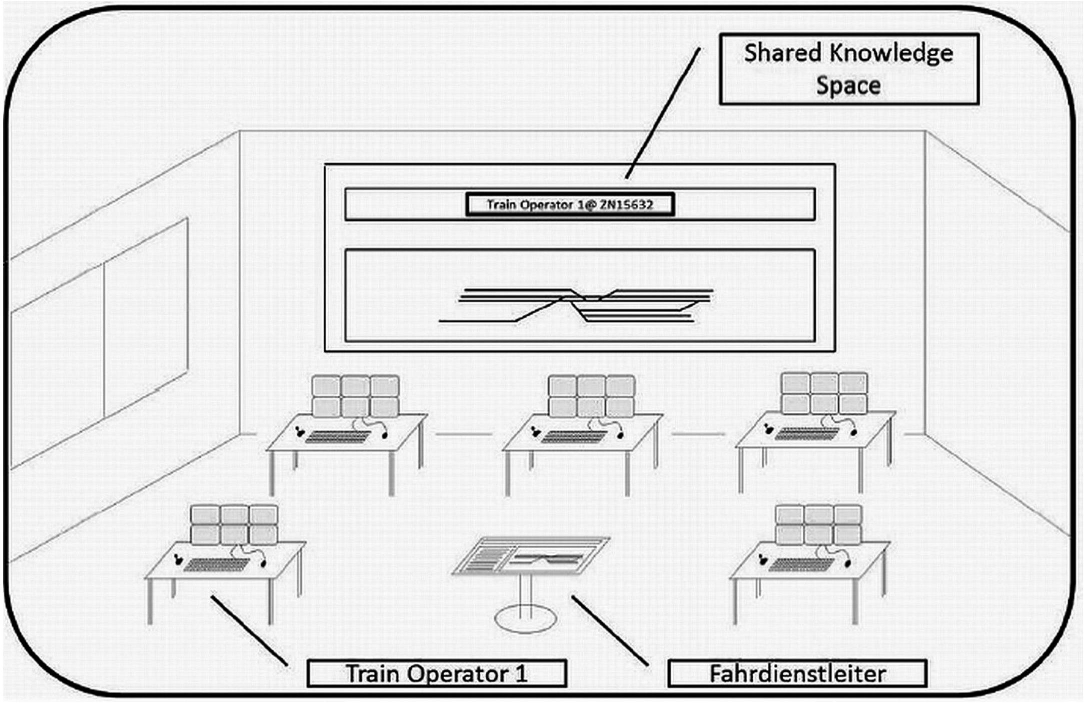


Figure 68: Schematic control room setting for train operators, copied from Brandenburger and Naumann (2018).

The shared knowledge space at the front depicts the entire area of operation with the following information:

- weather information,
- train status,
- current takeover requests.

The displays of the remote control workstations show information like train identity, speed requirements, schedule, live stream camera video, and the technical diagnosis of the on-board systems. Initially it was planned to assign several trains to one operator. But after some evaluation, this idea was changed to a "one TO – one train" paradigm (Brandenburger, Naumann 2018).

Figure 69-A shows the screen layout for the train operator (TO) in automatic mode, when the TO has to perform monitoring tasks. The screen provides:

- a zoomable overview,
- a schedule with specific regulations for the area of operation,
- a communication display.

Figure 69-B shows the screen layout for the train operator (TO) in manual mode, when the TO drives the train manually from the remote centre. The screen provides:

- live-stream video or additional video footage,
- the Driver Machine Interface (ETCS-DMI),
- the technical display (MTD),
- the schedule for the particular train,
- the reason for the manual takeover and the task.

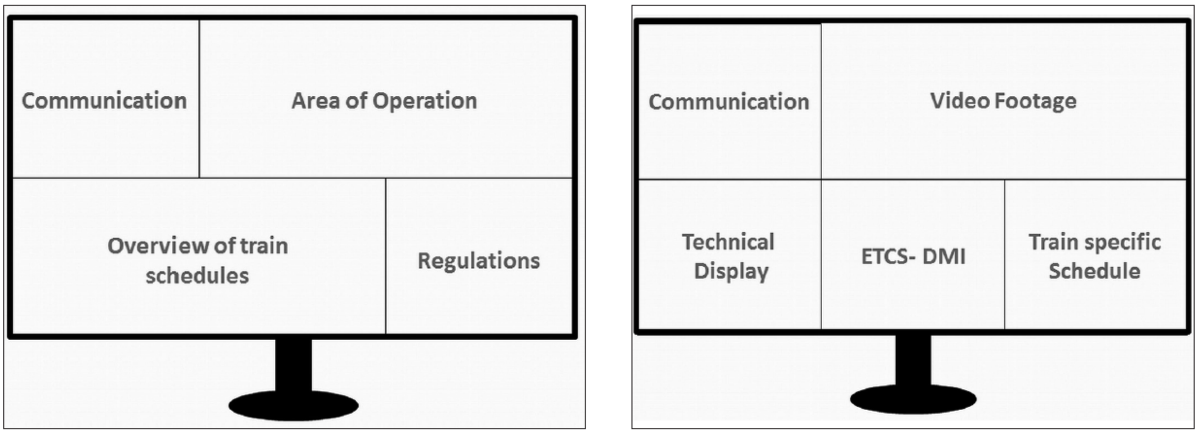


Figure 69: Screen layout for the train operator in automatic mode (A) and in manual mode (B), copied from Brandenburger and Naumann (2018).

Two further displays have been designed to support the transition of control: forward (automation to manual) and backward (manual to automation). Figure 70-A shows the forward transition interface. It provides:

- the reason for the takeover request,
- train specific information,
- a live video stream,
- an explicit acceptance mechanism which shifts the responsibility from the automation to the TO.

Figure 70-B shows the backward transition interface. It provides:

- a description of the task,
- a video,
- an acceptance mechanism for the transfer of responsibility back to the automation,
- a documentation of the initiated actions and outcomes for operational transparency and train status logging.

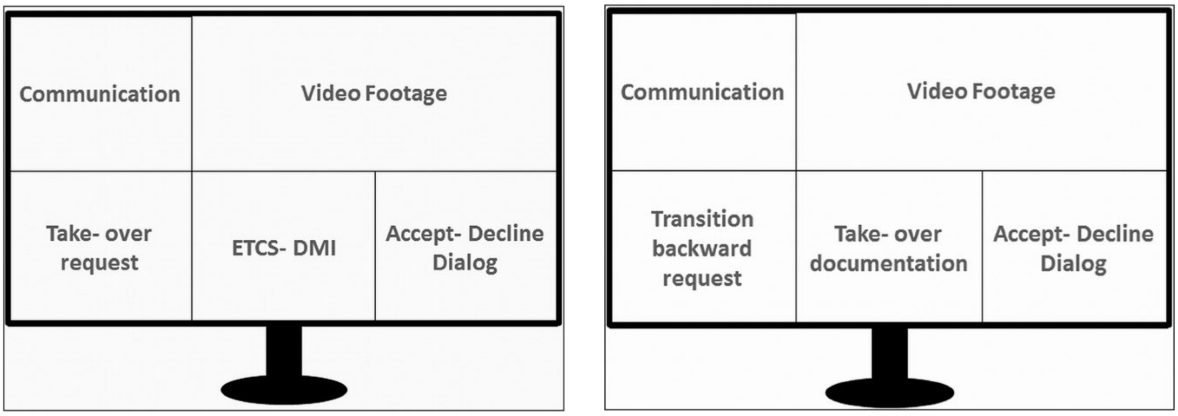


Figure 70: Screen layout for transition of control: forward (A) - automation to manual, and backward (B) - manual to automation, copied from Brandenburger and Naumann (2018).

13.4.3 Which legal aspects have been considered?

ARTE will investigate which steps are necessary for acceptance of autonomous trains and remote control concepts by the certification authorities. At the time when the State-Of-The-Art report was finalised, these results were not yet available.

13.4.4 Statements and Findings

Nr.	Statement / Finding	Source	Category
SoA-AR-1	An attendant working onboard the automated vehicle (e.g., taking care of passengers) could have a specific role in emergency situations.	ARTE	C1
SoA-AR-2	An attendant working onboard the automated vehicle (e.g., taking care of passengers) can support the remote operator.	ARTE	C1
SoA-AR-3	Specific screen layouts should be defined supporting automated and manual mode.	ARTE	C3
SoA-AR-4	Specific screen layouts should be defined supporting transfer of control from automation to human (e.g., the reason for the takeover request should be shown) and back (e.g., a documentation of the initiated actions and outcomes for operational transparency and train status logging should be shown).	ARTE	C3

14. Literature

Adebar, F.-A.; Milius, B. and Naumann, A. (2023). Flexible Arbeitsumgebungen für die ATO Rückfallebene. EI - Der Eisenbahningenieur, 01/23, Seiten 39-41. Tetzlaff Verlag.

Alsos, O. A.; Veitch, E.; Pantelatos, L.; Vasstein, K.; Eide, E.; Peterman, F.; Breivik, M. (2022). NTNU Shore Control Lab: Designing shore control centres in the age of autonomous ships. In Journal Phys.: Conference Series.

American Bureau of Shipping (2018). ABS Guide for Cybersecurity Implementation for the Marine and Offshore Industries - ABS CyberSafety™ Volume 2, 2018.

Ando, H.; Kuwahara, S.; Kutsuna, K.; Nakamura, J. (2022). Development and Demonstration of Autonomous Ship in Japan. Presentation given at the World Maritime Technology Conference (WMTC2022). URL: https://monohakobi.e-secure.co.jp/ja/wp-content/uploads/2022/08/20220428_WMTC-NYK-Ando_v.pdf (visited 22. Feb. 2023)

AutoShip consortium (2022). Autoship Newsletter. Issue No. 6, 25th February 2022. URL: https://www.autoship-project.eu/wp-content/uploads/2022/02/Autoship-Newsletter06.pdf (visited 28. Feb. 2023).

Bargsten, J., Schippers, M. (2022). Joint project between SEAFAR and HGK Shipping. Presentation given at ADN Safety Committe 40th Session.

Barrado, C.; Boyero, M.; Brucculeri, L.; Ferrara, G.; Hately, A.; Hullah, P.; Martin-Marrero, D.; Pastor, E.; Rushton, A.P.; Volkert. (2020). U-Space Concept of Operations: A Key Enabler for Opening Airspace to Emerging Low-Altitude Operations. In Aerospace 7, No. 3: 24.

Bejaoui, A.; F; Söffker, D. (2022). Supervision concept for situated human driving applied to inland shipping. IEEE International Conference on Intelligent Transportation Systems (IEEE ITSC 2022), Macau, China.

BIMCO et al. (2018). The Guidelines on Cyber Security Onboard Ships. URL: https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships (visited 22. Feb. 2023).

Bolbot V.; Theotokatos, G.; Faivre, J.; Wennersberg L.A.L, et al. (2021). AUTOSHIP deliverable D2.4: Riskassessments, fail-safe procedures and acceptance criteria". Technical report. URL: https://www.researchgate.net/publication/361738313_D24_Risk_assessments_fail-safe_procedures_and_acceptance_criteria_WP_n_and_title_WP2_-Scenarios_assessment_and_identification_of_gaps_and_barriers_for_scale-up (visited 28. Feb 2023)

Bolbot, V.; Theotokatos, G.; Boulougouris, E.; Vassalos, D. (2020a). Safety related cyber-attacks identification and assessment for autonomous inland ships. In Proceedings of the International Seminar on Safety and Security of Autonomous Vessels (ISSAV) and European STAMP Workshop and Conference (ESWC), Sciendo , 2020, pp. 95-109.

Brandenburger, N.; Naumann, A. (2018). Enabling automatic train operation through human problem solving. SIGNAL + DRAHT, 3, pp. 6-13. DVV Media Group.

Bureau Veritas (2019). Guidelines for Autonomous Shipping. NI 641 DT R01E. Paris: Bureau Veritas.

Bureau Veritas (2022). Bureau Veritas delivers an AIP for fully autonomous ship framework. News on website of Bureau Veritas. URL: https://marine-offshore.bureauveritas.com/newsroom/bureau-veritas-delivers-aip-fully-autonomous-ship-framework (visited 03. March 2023).

Collart-Dutilleul, S.; Levomte, T.; Romanovsky, A. (2019). Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification. Proceedings of the Third International Conference, RSSRail 2019, Lille, France

CORUS Consortium (2019a). Concept of Operations for European UTM Systems, Final Version. URL: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5c8b46d99&appId=PPGMS (visited 20. July 2023)

CORUS Consortium (2019b). Concept of Operations for European UTM Systems, Enhanced Overview. URL: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5c8b46d99&appId=PPGMS (visited 20. July 2023)

CORUS Consortium (2019c). U-space ConOps Annex D1: MEthoDology for the Uspace Safety Assessment (MEDUSA). URL: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5c8b46d99&appId=PPGMS (visited 20. July 2023)

DEME (2019). DEME deploys autonomous plastic collector on the river Scheldt. Artciöle on campany website. URL: https://www.deme-group.com/news/deme-deploys-autonomous-plastic-collector-river-scheldt (visited 06. March 2023).

DTT Consortium (2022). Final Project Report. URL: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5fcfea05b&appId=PPGMS (visited 06. July 2023).

Dybvik, H.; Veitch, E.; Steinert, M. (2020). Exploring challenges with designing and developing shore control centres (SCC) for autonomous ships. Proceedings of the Design Society: DESIGN Conference, 1, pp. 847 - 856.

Endsley, M.R. (1995). Toward a theory of situation awareness in dynamic systems. Human Factors. 37(1): 32–64.

EUROCAE (2020). Minimum Aviation Systems Performance Standards for Remote Pilot Stations conducting IFR Operations in Controlled Aispace (ED-272), EUROCAE, 2020.

European Maritime Safety Agency (2020a). SAFEMASS Study of the risks and regulatory issues of specific cases of MASS – Part 1.

European Maritime Safety Agency (2020b). SAFEMASS Study of the risks and regulatory issues of specific cases of MASS – Part 2.

European Maritime Safety Agency (2023). Risk-based Assessment Tool for MASS (RBAT) - Specific MASS concepts and risk evaluation technique proposed for testing the RBAT– Third report.

European Union (2019a). Commission Implementing Regulation. (EU) 2019/947 of 24 May 2019 on the Rules and Procedures for the Operation of Unmanned Aircraft. EU: Brussels, Belgium. URL: https://eurlex.europa.eu/legal-content/EN/TXT/?qid=1560259925294&uri=CELEX:32019R0947 (visited 01. Aug. 2023).

European Union (2019b). Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems. EU: Brussels, Belgium. URL: https://eur-lex.europa.eu/legalcontent/EN/TXT/?qid=1560259925294&uri=CELEX:32019R0945 (visited 01. Aug. 2023).

Friedrich, M., Timmermann, F., Jakobi, J. (2021). Supervising Multiple Remote Tower Operations: How to Develop and Test a New Work Position in the ATC Domain? In D. Harris and W.-C. Li (Eds.): HCII 2021, LNAI 12767, pp. 130–141. Springer Nature Switzerland AG

Friedrich, M., Timmermann, F., Jakobi, J. (2022). Active Supervision in a Remote Tower Center: Rethinking of a New Position in the ATC Domain. In D. Harris and W.-C. Li (Eds.): HCII 2022, LNAI 13307, pp. 265–278. Springer Nature Switzerland AG

German Federal Ministery of Digital and Transport (2023). Distinguishing between categories of operation. Digital Platform for Unmanned Aviation. URL: https://www.uas-operations.de/homepage/en/information/categorizing-drone-operations/distinguishing-between-categories-of-operation (visited 20. July 2023).

Hoem, Å.S.; Veitch, E.; Vasstein, K. (2022). Human-centred risk assessment for a land-based control interface for an autonomous vessel. WMU J Marit Affairs 21, pp. 179–211.

Hull to Hull Consortium (2018). H2H Concept Description.
URL: https://cordis.europa.eu/project/id/775998/results visited (visited 28. Feb. 2023).

IMO (2018). Regulartory Scoping Exercise for the Use of Maritime Autonomous Surface Ships (MASS). MSC 100/5/6. Comments on document. Submitted by Australia, Denmark, Finland, France and Turkey.

IMO (2019). Interim Guidelines for MASS trials.
URL: https://wwwcdn.imo.org/localresources/en/MediaCentre/HotTopics/Documents/MSC.1-Circ.1604%20-%20Interim%20Guidelines%20For%20Mass%20Trials%20(Secretariat).pdf (visited 08. March 2023).

IMO (2021). Outcome of the Regulatory Scoping Exercise for the Use of Maritime Autonomous Surface Ships (MASS). URL: (visited 08. March 2023).

INVIRCAT Consortium (2021). INVIRCAT Initial CONOPS - RPAS in the TMA. URL: https://www.invircat.eu/deliverables (visited 25. July 2023)

INVIRCAT Consortium (2022a). D3.4 INVIRCAT Exploratory Research Validation Report. URL: https://www.invircat.eu/deliverables (visited 25. July 2023)

INVIRCAT Consortium (2022b). INVIRCAT Final Operational and Technical Requirements Definition. URL: https://www.invircat.eu/deliverables (visited 25. July 2023)

Johnsen, S.O.; Bjørkli, C.; Steiro, T.; Fartum, H.; Haukenes, H.; Ramberg, J.; Skriver, J. (2008). CRIOP®: A scenario method for Crisis Intervention and Operability analysis. . SINTEF Technology and Society Safety and Reliability.

Kaarstad, M.; Braseth, A. O. (2020). Operating autonomous ships remotely from land-based operation centers: The current state-of-the-art. IFE/E-2020/008. Institute for Energy Technology, Halden, Norway.

Kongsberg Maritime (2021). Remote operation center. Video on Youtube. URL: https://www.youtube.com/watch?v=UPtdgiIrlJI (visited 27. Feb. 2023).

Kretschmann, L.; Rødseth, Ø.; Tjora, Å.; Sage Fuller, B.; Noble, H. (2015). MUNIN Project - Maritime Unmanned Navigation through Intelligence in Networks, Deliverable D9.2: Qualitative assessment. Technical Report. URL: (visited 15. Feb. 2023).

Lamm, A. (2022). AVATAR - modal shift from road to water. Project presentation. URL: http://alamm.de/wordpress/wp-content/uploads/2022/02/AVATAR-modal-shift-from-road-to-water.pdf (visited 08. March 2023).

Lamm, A.; Piotrowski, J.; Hahn, A. (2022). Shore based Control Center Architecture for Teleoperation of Highly Automated Inland Waterway Vessels in Urban Environments. In Proceedings of the 19th International Conference on Informatics in Control, Automation and Robotics, Lisbon, Portugal, 2022, pp. 17–28.

Live Sail Die (2022). Mahi 2 is the first autonomous vessel to cross the Atlantic. Article on the news webpage. URL: https://www.livesaildie.com/mahi-2-is-the-first-autonomous-vessel-to-cross-the-atlantic (visited 06. March 2023).

MacKinnon, S.N.; Man, Y.; Baldauf, M. (2015). MUNIN Project - Maritime Unmanned Navigation through Intelligence in Networks, Deliverable D8.8: Final Report: Shore Control Centre. Technical Report. CTH: Gothenburg, Sweden; HSW: Rostock-Warnemünde, Germany.

Maritime Executive (2022). Design for Autonomous, Zero-Emission Cross-Channel Vessel Obtains AiP. News article in the Online Journal. URL: https://maritime-executive.com/article/design-for-autonomous-zero-emission-cross-channel-vessel-obtains-aip (visited 03. March 2023).

Maritime UK (2018). Maritime Autonomous Surface Ships UK Code of Practice. Version 2.

MASS World (2022). SEAFAR is expanding to Germany. Blog article. URL: https://massworld.news/seafar-expanding-germany (visited 03. March 2023).

MUNIN Consortium (2015). Navigational shore support: A new perspective. Presentation at the MUNIN Final Event. URL: http://www.unmanned-ship.org/munin/wp-content/uploads/2015/06/MUNIN-Final-Event-B-4-CTH-MUNINs-Shore-Control-Centre.pdf (visited 07. March 2023).

Murray, B.; Rødseth, Ø. J.; Nordahl, H.; Lien Wennersberg, L. A.; Pobitzer, A.; Foss, H. (2022). Approvable AI for Autonomous Ships: Challenges and Possible Solutions. In Maria Chiara Leva, Edoardo Patelli, Luca Podofillini, and Simon Wilson (eds), Proceedings of the 32nd European Safety and Reliability Conference (ESREL 2022). Singapore: Research Publishing.

Nakashima, T.; Kutsuna, K.; Kureta, R.; Nishiyama, H.; Yanagihara, T.; Nakamura, J.; Ando, H.; Murayama, H.; Kuwahara, S. (2022). Model-Based Design and Safety Assessment for Crewless Autonomous Vessel. Journal of Physics: Conference Series 2311 (2022) 012024

Nakashima, T.; Kutsuna, K.; Kureta, R.; Nishiyama, H.; Yanagihara, T.; Nakamura, J.; Ando, H.; Murayama, H.; Kuwahara, S. (2019). NYK's Approach for Autonomous Navigation – Structure of Action Planning System and Demonstration Experiments. Journal of Physics: Conference Series 1357 (2019) 012013.

NIST (2018). Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. National Institute of Standards and Technology.

Note, P-J. (2022). MAHI – Project Mahi. Presentation given at the MASS Think Tank session on 28. Aperil 2022. URL: https://mass.kbrv.be/mass-sessions/project-mahi (visited 06. March 2023).

Pauwelyn, A-S.; Turf, S. (2023). Smart Shipping on Inland Waterways. Y. Li et al. (Eds.): PIANC 2022, LNCE 264, pp. 951–958.

Peeters, G.; Yayla, G.; Catoor, T.; Van Baelen, S.; Afzal, M.R.; Christofakis, C.; Storms, S.; Boonen, R.; Slaets, P. (2020). An Inland Shore Control Centre for Monitoring or Controlling Unmanned Inland Cargo Vessels. *Journal of Marine Science and Engineering*. 2020; 8(10):758.

Porathe T. (2021). Human-Automation Interaction for Autonomous Ships: Decision Support for Remote Operators. TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation, Vol. 15, No. 3, pp. 511-515.

Porathe, T. (2014). Remote Monitoring and Control of Unmanned Vessels: The MUNIN Shore Control Centre. Proceedings of the 13th International Conference on Computer Applications and Information Technology in the Maritime Industries (COMPIT '14), 12-14 May 2014 in Redworth, UK . V. Bertram (Ed.) Hamburg, Technische Universität Hamburg- Harburg.

Porathe, T. (2022). Remote Monitoring of Autonomous Ships: Quickly Getting into the Loop Display (QGILD). In: Katie Plant and Gesa Praetorius (eds) Human Factors in Transportation. AHFE (2022) International Conference. AHFE Open Access, vol 60. AHFE International, USA.

Porathe, T.; Fjortoft, K.; Bratbergsengen, I.-L. (2020). Human Factors, autonomous ships and constrained coastal navigation. The 3rd International Conference on Maritime Autonomous Surface Ship (ICMASS 2020) IOP Conf. Series: Materials Science and Engineering 929 (2020) 012007, IOP Publishing.

Rødseth, Ø.J.; Lien Wennersberg, L.A.; Nordahl, H. (2022). Towards approval of autonomous ship systems by their operational envelope. J Mar Sci Technol 27, üü. 67–76.

Rolls-Royce (2016). Rolls-Royce future shore control centre. Video on Youtube. URL: https://www.youtube.com/watch?v=ALwx5VP8kWA (visited 27. Feb. 2023).

Rolls-Royce (2018). Rolls-Royce and Finferries demonstrate world's first Fully Autonomous Ferry. News article from the Rolls-Royce website. URL: https://www.rolls-royce.com/media/press-releases/2018/03-12-2018-rr-and-finferries-demonstrate-worlds-first-fully-autonomous-ferry.aspx (visited 27. Feb. 2023).

Rüssmeier, N.; Lamm, A.; Hahn, A. (2019). A generic testbed for simulation and physical-based testing of maritime cyber-physical system of systems. Journal of Physics: Conference Series, 1357(1).

Safari, F.; Sage, B. (2013). MUNIN Project - Maritime Unmanned Navigation through Intelligence in Networks, Deliverable 7.2: Legal and Liability Analysis for Remote Controlled Vessels. Technical Report. http://www.unmanned-ship.org/munin/wp-content/uploads/2013/11/MUNIN-D7-2-Legal-and-Liability-Analysis-for-Remote-Controlled-Vessels-UCC-final.pdf.

SESAR Joint Undertaking (2017). U-space Blueprint. URL: https://www.sesarju.eu/sites/default/files/documents/reports/U-space%20Blueprint%20brochure%20final.PDF (visited 20. July 2023)

Smart Maritime Network (2022). Unmanned vessel control centre opens in Antwerp. Article on the Open Data Platform. URL: https://smartmaritimenetwork.com/2022/02/22/unmanned-vessel-control-centre-opens-in-antwerp (visited 03. March 2023).

Specht, F.; Michels, A.; Adebahr, F.-A.; Meirich, X. Hofstädter, R.; Milius, B.; Naumann, A. (2022). Automated driving in Lower Saxony – ARTE- SIGNAL + DRAHT (114), pp. 10-15. DVV Media Group. URL: https://elib.dlr.de/188466/1/2022_Signal%2BDraht_ARTE.pdf (visited 25. July 2023)

Veitch, E.; Alsos, O.A. (2021). Human-Centered Explainable Artificial Intelligence for Marine Autonomous Surface Vehicles. Journal of Marine Science and Engineering, 9, 1227.

European Maritime Safety Agency
Praça Europa 4
1249-206 Lisbon, Portugal
Tel +351 21 1209 200
Fax +351 21 1209 210
emsa.europa.eu