

## Article

# Engineer-Centred Design Factors and Methodological Approach for Maritime Autonomy Emergency Response Systems

Fredrik Asplund <sup>1,\*</sup>  and Pernilla Ulfvengren <sup>2,†</sup> <sup>1</sup> Department of Machine Design, KTH Royal Institute of Technology, 100 44 Stockholm, Sweden<sup>2</sup> Department of Industrial Economics and Management, KTH Royal Institute of Technology, 100 44 Stockholm, Sweden; pernilla.ulfvengren@indek.kth.se

\* Correspondence: fasplund@kth.se; Tel.: +46-8-790-7405

† These authors contributed equally to this work.

**Abstract:** Commercial deployment of maritime autonomous surface ships (MASSs) is close to becoming a reality. Although MASSs are fully autonomous, the industry will still allow remote operations centre (ROC) operators to intervene if a MASS is facing an emergency the MASS cannot handle by itself. A human-centred design for the associated emergency response systems will require attention to the ROC operator workplace, but also, arguably, to the behaviour-shaping constraints on the engineers building these systems. There is thus a need for an engineer-centred design of engineering organisations, influenced by the current discourse on human factors. To contribute to the discourse, think-aloud protocol interviewing was conducted with well-informed maritime operators to elicit fundamental demands on cognition and collaboration by maritime autonomy emergency response systems. Based on the results, inferences were made regarding both design factors and methodological choices for future, early phase *engineering* of emergency response systems. Firstly, engineering firms have to improve their informal gathering and sharing of information through gatekeepers and/or organisational liaisons. To avoid a too cautious approach to accountability, this will have to include a closer integration of development and operations. Secondly, associated studies taking the typical approach of exposing relevant operators to new design concepts in scripted scenarios should include significant *flexibility* and *less focus on realism*.

**Keywords:** maritime autonomy; emergency response; maritime autonomous surface ship (MASS); remote operations centre (ROC); safety; cognitive systems engineering; human-centred design; engineer-centred design



**Citation:** Asplund, F.; Ulfvengren, P. Engineer-Centred Design Factors and Methodological Approach for Maritime Autonomy Emergency Response Systems. *Safety* **2022**, *8*, 54. <https://doi.org/10.3390/safety8030054>

Academic Editor: Raphael Grzebieta

Received: 1 May 2022

Accepted: 19 July 2022

Published: 29 July 2022

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

Commercial deployment of maritime autonomous surface ships (MASSs) is close to becoming a reality, and the context and operating conditions of MASSs are receiving an increasing amount of attention [1–4]. The related definitions of levels of automation typically include a highest level at which no remote operations centre (ROC) operator actively monitors the automatic decision-making of the MASS [1,3,5]. Nonetheless, this is only part of the truth. Even fully autonomous ships will allow ROC operators to take over control during an emergency [6]. Who will be able to take over control, and thus act as a ROC operator, is still not defined. Depending on future regulation, these operators could work at centres owned by, for instance, private shipping companies or public vessel traffic services providers. However, given the dependability required of autonomous systems, these emergencies will be rare exceptions. It is thus very likely that the ROC operators responding to them will face many of the same problems related to “clumsy automation” that transitions between other levels of automation have faced in other domains [7,8]. It would thus likely be valuable if human-centred design factors could be identified for maritime autonomy emergency response systems, i.e., aspects of, for instance, organisations

or interactions that can be purposely structured to avoid automation-related problems. These factors would require many aspects of the future context surrounding these systems to be analysed, related to future demands on, e.g., cognition, training and organisational contexts [4].

Human factors is a core field of study that addresses such aspects by following technology development and relating human knowledge to operator–machine or socio-technical systems. Numerous methods and tools from human factors have been used in field studies and intervention projects to reveal specific needs in various work contexts and environmental settings [9]. Human factors research has traditionally suggested that these problems should be addressed by engineers during the system design phase through a more complete, human-centred consideration of operator–machine interactions. However, safety is a critical system property that is meticulously handled through the system life cycle. If an *autonomous* system is not able to at least bring itself to a safe state during an emergency, then the situation is by definition beyond what its engineers could even *envision* during system construction. If the hazard itself has not been overlooked, then at the very least the full implications of the hazard have been misunderstood. In other words, operators will by definition find themselves handling a MASS encountering an *unknown unknown*, i.e., what engineers would consider an unknown unsafe scenario [10]. A completely unforeseen situation might end up pitting the system against operators, rather than allowing it to help the operators in carrying out their tasks. Add to this the aforementioned complex aspects, and the engineering task of assuring a safe, human-centred design becomes impossible.

It is argued here that traditional human-centred design processes, standards and guidelines are unfit for the task of supporting systems and safety engineers in designing a system tailored for operators in situations which neither engineers nor operators have anticipated. Rather than only defining design factors for the operational context, the focus should thus also be on suitable design factors for engineering work activities. All work environments can be designed with a human-centred approach, even those of the *engineers* designing complex systems such as MASSs and ROCs. In other words, if engineers cannot *always guarantee* a suitable match between the design of a MASS, and the abilities of ROC operators, then the context in which engineers work might have to be designed to improve their ability to identify and react to unforeseen difficulties faced in operations. Unfortunately, this is made difficult by the *envisioned world problem* [11,12], i.e., the difficulty in designing work systems for a future in which practice has changed substantially. Waiting for flag states and the International Maritime Organisation (IMO) to first set detailed operational constraints for responding to MASS emergencies might be tempting. However, this will limit the possibility to proactively influence these constraints, and the associated engineering practice.

Therefore, this study utilizes early stage simulations to identify fundamental demands on operators by maritime autonomy emergency response systems. These demands are used to infer and discuss what constitutes the appropriate design factors for the engineering of maritime autonomy emergency response systems. Furthermore, observations from the applied research methodology are also used to infer recommendations for methodological choices when researchers and engineers attempt this type of study. This clarifies and extends what “human-centred design” can mean for maritime autonomy emergency response systems, and gives engineers and researchers the tools for early investigations into these systems.

Section 2 presents the theoretical background of the study, which Section 3 builds upon to motivate and describe the methodology used. Section 4 outlines and analyses the results of the study, before Section 5 discusses the related implications as well as their limitations. The paper ends with Section 6 summarizing the conclusions of the study.

## 2. Theoretical Background

This section provides the theoretical background of the study based on the discourse on cognitive systems engineering. Firstly, this allows us to discuss the relationship between

human factors and both the operations involving complex cyber–physical systems (CPSs) and the engineering to bring about these operations. Secondly, it allows us to suggest that the engineering of complex CPSs might benefit if human-centred design is not only applied during, but also to, engineering activities. Both perspectives are elaborated on in Section 5 to clarify the implications of this study for early investigations into emergency response systems for autonomous vehicles.

### 2.1. (Cognitive Systems) Engineering

Various terms are used to discriminate between the focus of design and work systems. The term cognitive systems engineering [13] originally refers to the development of methods and tools for developing cognitive systems, i.e., systems supporting decision making and problem solving. Although the aim is overall system performance and the systems consist of both humans and technology, the focus has been to define requirements supporting the human or user [9]. According to (cognitive systems) engineering ((CS)E), it is possible to design an embodiment relation with technology, in which a system becomes intuitive and usable through technology enhancing human capabilities and reducing operator limitations [13,14]. Still, it is important to note that this is not only a matter of simplifying systems—the law of requisite variety implies that effective control is impossible if, e.g., a maritime autonomy emergency response system has less variety than the MASS itself [15]. An oversimplified system can easily lead to a hermeneutic man–machine relation [16], in which the operator has to cope with the variety of both systems.

The implication is that human-centred design factors should be defined for CPS operations involving operators, lest systems are designed that do not take the individual abilities and limitations of operators into account. Otherwise, the result can, e.g., be a remote control that hinders rather than supports a ROC operator trying to handle a MASS emergency.

Unfortunately, despite the ambition to develop holistic and truly computer-integrated systems, such efforts have historically often merely resulted in computer-interfaced systems [17]. This distinction was repeated in later writings on joint cognitive systems [13]. The guiding principles for engineers that derived from this era of research and technology was aimed to mitigate problems resulting from a failure to design systems that took the human sufficiently into account. By contrast, less human-centred practitioners, engineers and researchers were perceived to fail to fully realise the importance of functional boundaries, weaknesses of the system or resource deficits in operations. Symptomatic of this perception was often to define system failures as “human error” and blame the user for using tools, equipment or systems in the wrong way. Research provided the engineering community with automation-related design concepts and guidelines with warning examples of consequences when human-centred approaches had not been sufficiently applied, such as “ironies of automation” [7], “clumsy automation” [18], “automation induced surprises” [19] and “situation awareness” [20]. Nevertheless, these design concepts and guidelines have not been translated from the human factors community to the actual methods used by the engineering community. There is thus a lack of support for decision making and problem solving early in the system design cycle for technical solutions that will reduce the human operator’s exposure to undesired situations in operations.

### 2.2. Safety and Systems Engineering

As systems have become more complex, the human-centred design concepts have provided a broader scope to traditional interface design [16]. A user-centred design approach is based on the assumption that design starts with the activity of the user, and the only reasonable way to capture user needs is to incorporate the user into the design process. The general principle is to elicit relevant user requirements, goals and tasks to define system specifications utilizing the value of know-how and established work practices [17]. After a concept has been developed this can be followed by usability testing. These perspectives on a design rooted in the abilities of the user of the system, and that “human error” can be

induced by the operational context, have strongly influenced safety engineering. Unfortunately, although this has increased the awareness of usability and safety in operations, this approach does not necessarily support the identification and mitigation of flaws in the technical design; the argument being that although technical weaknesses will be manifested in incidents, if the cause of the incident included a technical design flaw, then the user, a victim under the circumstances, will not have feedback on how to fix the technical flaw. At most, the aforementioned design concepts and guidelines help build a buffer to technical failures, but do not support the technical systems engineering that could resolve core issues in the original designs. This suggests that the scope of system engineering for safety has to be enlarged [21].

Principles behind, for instance, (CS)E must be adopted by engineers in engineering processes producing complex, safety-critical socio-technical systems [21]. This extension of the scope of human-centred design to engineering processes suggests that *system engineers* should ensure that engineering activities take care to address the implications on operations by *complex socio-technical systems* [22]. This has had a particularly strong impact on the engineering specifications generated through the *requirements engineering* process. In other words, human-centred design has implications for engineering processes.

Simultaneously, that contemporary system complexity has reached a point at which all the potential interactions among system components cannot be anticipated, identified, and guarded against has emerged as an underlying assumption in contemporary systems engineering focusing on complex socio-technical systems. Rather than spending time on each interaction, engineers should shift their focus to the *constraints* that limit these interactions. Engineers have historically made use of models of causation in safety engineering that build on individual faults. A shift towards constraints suggests the need to rather use models of causation from systems theory [23], as well as relevant theory on communication and control such as hierarchy theory [24] and hierarchical control [25]. This is well aligned with the systemic approach of human factors research.

Safety engineering and, e.g., (CS)E have thus moved the safety-related requirements process towards a focus on ensuring suitable constraints during operation. After this requirements engineering process, when *constraints* required to ensure safety have been identified, they will be addressed by engineering processes meant to ensure the development of a safe product. The principles for which these processes work can be summarized as [26]: (1) requirements will have to be created that describe how different system components help enforce the constraints; (2) the intent of these requirements will have to be maintained as they are decomposed into lower levels of requirements that can be directly implemented; (3) engineers have to demonstrate that the requirements have eventually been satisfied; (4) any negative, additional effects introduced by the constraints or their implementation have to be handled; (5) engineers have to apply these principles in a way that ensures confidence commensurate to the risk to be mitigated by the constraints. System engineering is the engineering discipline tasked with ensuring that system properties such as safety are handled according to these principles. Undoubtedly, the systems engineering methods and models applied to this task have shown themselves to be both important and necessary [27,28].

Human factors are also explicitly related to this systems engineering practice through process descriptions meant to give guidance on how to act appropriately throughout a product's life cycle [29,30]. Arguably, the requirements engineering process is still the central part of this association between human factors and engineering practice. However, it is clear that this association favours an iterative return to and elaboration of risks and requirements [31]. This means that also processes that are carried out after system deployment have had guidance created for them that is relevant for human factors. Processes during, for instance, system utilization become important to ensure that operators can make engineers aware of difficulties faced during operations.

### 2.3. A (Cognitive) System Engineering?

However, this high level guidance is only a brief description and structuring of engineering activities, it is not a definition of how engineers actually carry out their work. Firms producing contemporary, complex products such as MASSs are typically split across several engineering disciplines that each constitute their own community of practice [32]. These communities are “groups of interdependent participants [that] provide the work context within which members construct both shared identities and the social context that helps those identities to be shared” [33]. As such they allow engineers to *in detail* learn and agree on acceptable engineering practice through networking and shared, often tacit, knowledge [34–36]. While at times communities make efforts to unify their practices, this is not only costly but also risks compromising each discipline’s engineering techniques [37].

Broad phenomena such as autonomy will thus most likely be approached through integration between disciplines, complicated by, e.g., differences in authority between their communities [32]. The situation is similar for researchers, who work in separate communities focused on specific research fields. Collaborative research has resulted in, e.g., broader, improved models for use by practitioners [38], but can also be hindered by conflict and differences between research disciplines [39].

In other words, guidance exists on which engineering activities could be carried out to consider difficulties with operating complex CPS, which stakeholders could be necessary in these engineering activities, and which (qualitative) methods could be used in them. Still, the quality of the output of these activities rather depend on the knowledge possessed by and integration of multiple engineering disciplines. This quality will be difficult to ensure when it is impossible to define constraints on the system to guarantee a suitable human–machine interaction, such as when the situation for which the system is being designed postulates the existence of unknown unknowns. (As, for example, when a ROC operator has to take emergency action due to a MASS facing a situation it is not designed for.) In these circumstances the ease of operating the system will only be as well designed as it can be if the involved stakeholders have sets of knowledge that are diverse enough, while they at the same time can understand each other well enough [40,41]. While communities of practice align their members and facilitate the existence of a diversity of knowledge inside a firm, they will also create barriers to knowledge transfer and a mutual understanding [42]. These barriers will always exist simply because people are different [43,44], but overcoming them when they are caused by boundaries between communities or organisations might require specific boundary spanners or artefacts [45,46].

This implies that the main challenge that needs to be overcome for designing maritime autonomy emergency response systems involving human operators might be how to obtain a diverse set of necessary stakeholders to engage with engineers, while also allowing them to understand each other sufficiently well. To handle this challenge also requires an understanding of the constraints on engineering firms rather than the products they build. The structure of the work domain, work tasks and strategies, social and organizational factors, worker competencies and physical environments are all behaviour-shaping constraints that affect engineers’ ability to perform their work with the required flexibility [47]. Therefore, it is not enough to appreciate the need for system engineers to help other engineers understand how to deal with socio-technical issues in their processes [22,48]. Instead the same socio-technical analyses should be applied to the interactions between engineering disciplines and other stakeholders to avoid only indirectly noticing associated difficulties with collaboration and communication.

Arguably, the engineering of complex CPSs might require system engineering able to apply *human-centred* design to engineering organisations and activities, i.e., an engineer-centred (*cognitive*) *system engineering*.

### 3. Methodology

This section provides a case description, and describes the study’s approach to data collection and data analysis.

### 3.1. Case Description

The study was conducted together with operators from the Swedish Maritime Administration (SMA) [49] and the Swedish Transport Administration (STA) [50]. Both SMA and STA are governmental agencies involved in the handling of, and long-term planning for, maritime operations.

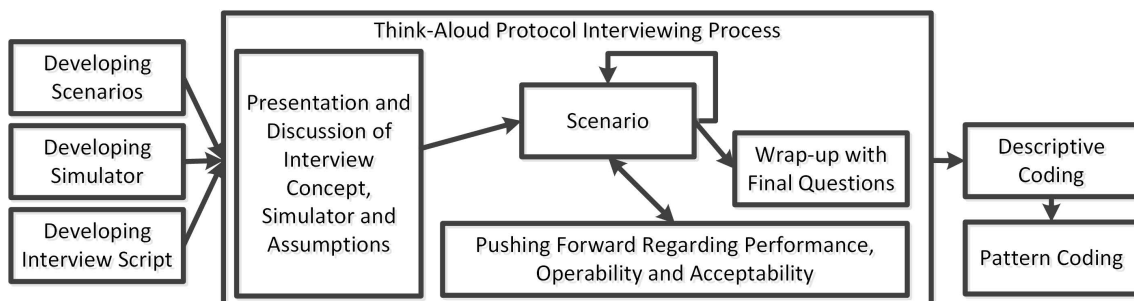
SMA is responsible for maritime safety and availability. Three important services provided by the SMA are pilotage, fairway services, and maritime traffic information. Specifically, SMA operates remote operations centres (ROC) to provide vessel traffic services (VTSs), which share maritime traffic information to help avoid collisions and improve navigational safety. This information, shared as warnings and advice, includes, e.g., the movement of ships, issues with maritime safety infrastructure, and weather conditions. Strategically, SMA has taken the initiative to start and participate in several research projects focusing on, e.g., maritime digitalisation, automation and information sharing. Although SMA is primarily focused on merchant shipping, the agency also keeps the interests of recreational crafts, commercial fishing boats and the Swedish Navy in mind during these activities.

STA responsibilities include operating the Swedish road ferries. This task involves ensuring their environmental sustainability [51]. STA is thus deploying technology that enables road ferries to be utilized on demand rather than according to static itineraries, and which can improve their use of resources through, for instance, navigational optimization. This means that STA has procured ferries that will eventually be capable of autonomous operation [52]. Furthermore, STA is responsible for leading the long-term planning of the Swedish maritime transportation system. Therefore, STA plans for the integration of different types of traffic in important geographical locations, and decides where harbours and other maritime infrastructure should be placed.

Operators from SMA and STA are thus among the most well-informed regarding the current status of the maritime transportation system in Sweden. Furthermore, they are also informed about the decision-making in both short- and long-term projects aimed at improving maritime infrastructure. In fact, for STA, this involves the earliest procurement and deployment of MASSs in Sweden and globally.

### 3.2. Data Collection and Analysis

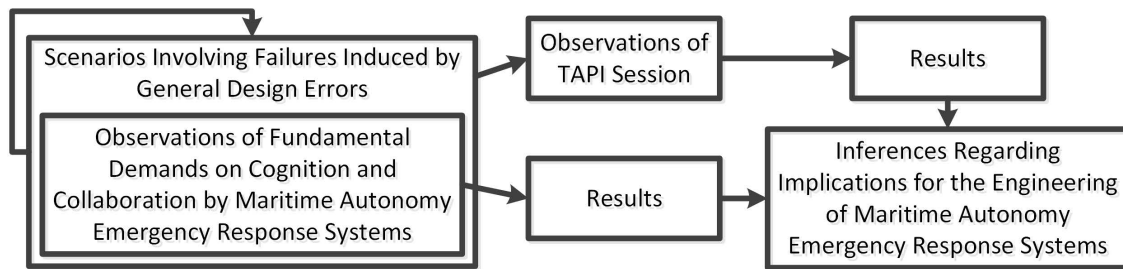
This subsection is divided into four parts. Firstly, we describe our preparations for the data collection. Secondly, we clarify some of the choices made during the preparation related to how the study approached the envisioned world problem. Thirdly, the implementation of the data collection is described. Finally, the data analysis is detailed. This data collection and analysis process is visualized in Figure 1.



**Figure 1.** The Data Collection and Analysis Process.

This process involved making observations regarding maritime autonomy emergency response systems and the methodologies that can be used to study these systems. These observations were then used to make inferences regarding the associated implications for the future engineering of maritime autonomy emergency response systems. This approach is visualized in Figure 2.

We refer to the individual subsections for the details of the process and the approach.



**Figure 2.** The Data Collection and Analysis Approach.

### 3.2.1. Data Collection Preparations

As described in the introduction, the goal was to study how to clarify and extend what “human-centred design” can mean for maritime autonomy emergency response systems, and to give engineers and researchers tools for early investigations into these systems. Both researchers [12,53,54] and practitioners [55] typically expose relevant operators to new design concepts to study the design of work systems for a future in which practice has changed substantially. This approach can be seen as putting forth novel work system designs as hypotheses for how an envisioned world will be constructed [56]. However, these design concepts can still be more or less complete, depending on which guidance is available and what type of answers are sought. At the time of this study, the introduction of MASSs is still at an early stage. There are no mature, well-defined design factors for maritime autonomy emergency response systems, and the demands these will put on engineering organisations are unknown. One can then *rather* seek to explore the fundamental demands on cognition and collaboration by developing scenarios that involve failures induced by general design errors [56]. This allows a researcher to rely less on the face validity of the design concept simulation, and instead lean on the relevance of the failures and the extent to which real problem-solving expertise is brought to bear on the scenarios. In such study designs, it is appropriate to collect data through ways that allow interviewers to study the thinking processes of interviewees. The technique used in this study was thus “think-aloud protocol interviewing” (TAPI) [57], i.e., probing interviewees with questions to get them to talk about their reasoning as they carry out tasks of interest.

Preparing for TAPI involves designing an interview script and preparing a suitable context for the think-aloud interviews.

The interview script was prepared according to the first steps of the procedure defined by Brinkmann and Kvale [58]. Firstly, this involved thematising the study. Two research questions were identified: the identification of design factors for such systems, and the identification of best practice when studying and designing such systems. Drawing on inspiration from the state-of-the-art and the European operational concept validation methodology (E-OCVM) [55], a one-page operator brief and a three-page interview script were prepared. Secondly, interview questions were formed based on the research questions. In addition to interview questions to be asked before and after the TAPI sessions, several follow-up questions were explicitly noted in the script. This ensured that the interviewers could “push/move forward” [58].

A professional traffic monitoring system was configured as a context for the TAPI. This involved automating 10 scenarios involving MASSs breaking down due to component failures, unexpected environmental factors or combinations of the two. The graphical user interface was centred around a sea chart, as this has been motivated for local operations and also for future traffic and fleet management [59]. Various surface ships, including the MASS monitored in the scenarios, were tracked together with their routes on the main sea chart. Operators could, by selecting an individual MASS, access panels with its charts, sensor data and health status. This situational awareness data and a visualization of the current health of a MASS could also be accessed in separate windows for detailed inspection. As

the scenarios progressed, warnings and alerts were provided to operators on the main sea chart. These provided information on phenomena which the MASS in the scenario deemed it could not handle with enough certainty.

The graphical user interface of the design concept simulation and the scenarios are described in Appendices A and B, respectively.

### 3.2.2. Methodological Choices

As mentioned in the previous subsection, this study developed scenarios that involved failures induced by general design errors [56]. The intent was not to evaluate the graphical user interface of the reconfigured traffic monitoring system. Instead, the investigation relied on bringing real problem-solving expertise to bear on the scenarios. Specifically, the focus was on how the operators would come to either accept or reject the behaviour of the MASS at hand. While the traffic monitoring system had to be realistic, it should not limit or confuse the actions that the operators envision themselves performing. Unfortunately, due to the envisioned world problem it is difficult to know how to enable an embodiment relationship, during TAPI, in which the operator is supplemented by the variety of the maritime autonomy emergency response system. The first methodological choice was thus related to *flexibility*.

Rather than providing all of the possibly relevant information in the graphical user interface, the focus was on the situational awareness and health of the monitored MASS. Other information that was requested by the operators was provided verbally by the interviewers. The only constraint was the narrative of the failure, i.e., the hazard in each scenario that was to be investigated. The idea was not to explicitly convey this narrative to the operators when additional information was requested. Instead, the operators were able to discuss the graphical user interface, or state that they were contacting other actors they deemed relevant. In this way, the interviewers could elicit where the operators believed important information related to MASS emergencies would be available, and what this information would consist of.

The second methodological choice was related to the realism of the TAPI sessions. The most fundamental choice is then related to how actively involved the interviewer should be during the interviews [60]. While less interaction could enhance realism, it would also make it more difficult to understand the reasoning of the operators correctly and completely. This trade-off makes it important to note the broad operational aspects that should be evaluated for future traffic management systems. E-OCVM [55] suggests that early feasibility evaluation can consider the performance, operability and acceptability of the human and technology integration, operating procedures, and communication requirements. Each such combination can be evaluated for guidance on interview questions for “pushing/moving forward” [58]. However, different combinations will be more or less important based on the concept and research questions involved in the study. Only the most important combinations should be followed through. To exemplify this, Table 1 identifies combinations deemed the most important for this study, and the associated cues used to develop interview questions for “pushing/moving forward”.

**Table 1.** E-OCVM operational aspect evaluation to guide interview script.

	Human and Technology Integration	Operating Procedures	Communications Requirements
Performance	A delay introduced by the operational concept.	Communication with irrelevant stakeholders.	A search for irrelevant information.
Operability	Confusion introduced by operational concept.		Not all relevant information sought.
Acceptability	Request for information not in operational concept.		



Arguably, asking these interview questions will detract further from the realism of the TAPI sessions. However, both clarifications and elaborations could reinforce the ability to explore the narratives of the scenarios.

### 3.2.3. Implementation of Interviews

The data collection took 4 months and involved 3-hour TAPI sessions with eight operators, characterized in Table 2. Within the limits of the case, the interviewees should be diverse enough to constitute a sample with good coverage. One session involved two interviewees, while the others involved one. The operator brief was sent to all interviewees before the interviews to allow them to prepare themselves. At the start of each interview, the operator brief and the traffic monitoring system used for the TAPI sessions were discussed with the interviewee. This minimized misunderstandings regarding the intent of the sessions. Each interviewee was subjected to a random set of three to five of the predefined scenarios. This ensured that each scenario was evaluated at least twice, and often more than three times.

**Table 2.** Interviewees.

Interviewee	Maritime Experience	Background
1	20+ years	Shipmaster's degree, Merchant Navy, Professional Maritime Education
2	5+ years	Shipmaster's degree, Vessel Traffic Services (VTSs)
3	25+ years	Shipmaster's degree, Navy, VTSs
4	10+ years	Shipmaster's degree, Offshore industry, Passenger traffic, VTSs
5	25+ years	Shipmaster's degree, Pilotage, VTSs
6	15+ years	Shipmaster's degree, Merchant Navy, VTSs
7	20+ years	Shipmaster's degree, Merchant Navy, Passenger traffic
8	15+ years	Maritime engineer, Passenger traffic

The interviewers needed to listen actively [58] to make sure that all ambiguous responses were clarified and all important leads were followed up on. To ensure this active listening, at least three interviewers and a technical support person were present at each session. The interviewers took turns to either ensure that the interview script was followed or focus on the interviewee's responses. The technical support person ensured that all interviews could be carried out as planned.

Video of all interviewers, the interviewees and the traffic monitoring system as used by the interviewees were recorded. As the aim was to capture the interviewees' thought processes on video, the predefined follow-up questions were used as reminders to verbalise. The interviewers kept a log of questions that were not fully answered. After the TAPI, information regarding any open issues, the interviewee's background and general thoughts on the session were gathered before the interview was ended. This included checking the relevance of the scenarios with the interviewees. All operators stated that the scenarios they were subjected to were highly relevant, and included risks likely to be found in a future maritime transportation system.

### 3.2.4. Data Analysis

The data analysis involved two phases. The first phase took three months, while the second phase was finished in one month.

In the first phase, all of the videos were coded and associated with journal notes from the TAPI sessions. Coding was related to sections of video, and summarized what took place in these. This was done separately by the authors to minimize the introduction of interviewer bias.

In the second phase, patterns were identified and summarized into findings. These patterns were discussed between the authors in relation to the video sections to arrive at

a common interpretation. This also meant that valid inferences could be drawn, even if the relevant sections were long and contained non-verbal communication. This concluded with relevant sections being transcribed with enough detail to, when relevant, capture the behaviour of the operator, the operator's actions as related to the expected narrative, and the progression of the scenario at hand. Based on these transcriptions, the phase ended with a discussion between the authors to agree on the results.

#### 4. Results and Analysis

This section describes the results from the study, i.e., the observations made during the TAPI sessions and the associated analysis. Firstly, regarding fundamental demands on cognition and collaboration by maritime autonomy emergency response systems considering their main role as support for ROC operators when a MASS encounters an unknown unknown; and secondly, regarding the methodological approach of both researchers and practitioners when studying and engineering such systems. The results are presented as quotes from the interviewees interspersed with analysis. These quotes are provided as *examples* of findings identified repeatedly throughout the TAPI sessions. As the scenarios were not used to test a new work system design, the outcomes of simulations were not deemed important. Observations regarding fundamental demands on cognition and collaboration were just as likely to occur when the interviewees failed to handle a scenario, as when they succeeded in doing so. Emphasis is added to some transcriptions to clarify the accompanying interpretation, as the actions and statements by the interviewees were at times contradictory. Furthermore, the points made and situations described in the quotes were in some cases sharpened by the interviewees to carry their message across to the interviewers. For example, the interviewee quoted in Section 4.1.1 does not necessarily think that a fifteen year old should be allowed to remotely operate a MASS during an emergency, but rather that maritime experience is not the most important qualifier for this work. Therefore, attention should be given to the provided analysis to avoid overinterpreting the quotes.

##### 4.1. On Fundamental Demands on Cognition and Collaboration

Three needs when designing for fundamental demands on cognition and collaboration are highlighted. Firstly, the need to design for domain experts. Secondly, the need to dynamically direct the attention of the ROC operators. Thirdly, the need to accept uncertain information sources.

###### 4.1.1. Design for Domain Experts

As it is difficult to ensure efficient constraints on a situation in which a MASS is encountering an unknown unknown, the temporal and spatial distance to an accident can be small. According to the interviewees, the *minimal* requirement on a ROC operator would thus be the ability to identify and prioritize among hazards when automation fails to do so correctly. At the very least, a maritime autonomy emergency support system should thus be *designed for a maritime domain expert*. It is important to note that this is not necessarily an expert in specific (maritime) skills such as navigation, but rather in maritime hazards and environmental phenomena. In fact, the former skills would most likely be available remotely. Interestingly, some of the operators downplayed the expertise required to understand maritime hazards. However, during their TAPI sessions, they themselves repeatedly exemplified just how complex this reasoning can become.

*Interviewer:* Do you need a shipmaster's degree, and a few courses...

*Interviewee:* No, you don't need that. What we are doing here is a computer game. A fifteen year old can do it, *if he is interested* ... When things are happening, if this fifteen year old *sees that here there is a problem*, if this fifteen year old can bring in his expert team ... then he just calls and says ... or she of course ... that this is something we need to look closer at. Here there is something that can become a problem *according to the information I am getting here*.

The interviewees, and their actions, helped identify two associated challenges. Firstly, if the emphasis is on domain knowledge, situations could easily be interpreted as mundane even when a MASS has signalled risk. Either because the ROC operators do not have enough system knowledge, or because they have very strong mental models for how a maritime environment is best interpreted. As an example, several operators stated that ships meet all the time, and that a MASS will have to handle such situations without human intervention. However, in several instances they still did not pursue a clear warning from a MASS about this kind of situation by digging into exactly what the warning was about.

(Preceding discussion about what sensors and information are available, such as data from the Automatic Identification System (AIS). In the meantime the interviewee misses changes to the sensor data, but reacts when finally seeing the camera data.)

*Interviewee:* That is great. Perfect. Exactly what I want. So, there was a boat without AIS coming from there.

*Interviewer:* So, what would you have thought if you would have been alerted about a boat showing up.

*Interviewee:* No, that is alright ... that it was so close that it wanted to change course ...

(Small discussion about where in the interface the information was available, scrolling back and forth the interviewee indicates that *the information from the camera was the only thing* required to understand the situation.)

*Interviewee:* So, if the MASS has done that correction, then everything is fine. Then you don't need to do anything more.

*Interviewer:* Do you need to know anything more from the ship to decide if it was a correct course correction, or the right thing to do ...

*Interviewee:* No, not anything more than what preceded that ... that he created a new route ...

Secondly, ROC operators might be better than MASS designers at identifying risk. This is not a problem in itself, but it might prompt operators to take control of a MASS when risk is quite low. To avoid this it might be better to allow operators to provide cues on risks to a MASS, and allow the MASS to act on these risks themselves.

(The interviewee is alerted to a group of kayaks by a MASS. He dismisses them as they *should be* clearly recognizable on camera and radar.)

*Interviewer:* So, no need to worry?

*Interviewee:* No, I don't think so. Well, there could be ... what it could be ... but then I have to trust the sensors, and there is a warning. Perhaps one should be alert just afterwards ... no-one has stopped ... so that the course correction was not enough. So, they do not turn around. Perhaps they change their minds because they are worried. Then it is a new situation. So, because of that you can be on the lookout to make sure the situation is resolved. To help the system a bit ...

*Interviewer:* More like sending in information to indicate that one of the kayaks is hesitating, going back?

*Interviewee:* Yes, that I could for example have seen on the camera, or on the radar ... that one echo is going back .. they are splitting up ... and that is what could happen, that things do not play out like you thought it would. Then you need to help out a bit.

#### 4.1.2. Ensure a Dynamic, yet Appropriately Narrow, Focus

Naturally, a transparent or explainable reasoning by MASSs is thus important. These topics are also receiving more attention in the maritime context [61]. The interviewees

expressed an interest in such information pertaining to both short and long time perspectives. How information pertaining to a longer perspective will be shared in the future was unclear, but it was important to have it available as a basis for operators' assessments and support for non-autonomous traffic.

*Interviewee:* However, we provide feedback at every critical point on the map. It is very seldom that we do not provide feedback. We ask follow-up questions and provide feedback ... it is an area that requires a lot of ... we are more active with information and questions, this communication to help and assist the crews. We are very active.

*Interviewer:* And what is it that you typically help with?

*Interviewee:* We let them know who they are going to meet and *which intentions they have*. It is going to take that way, or that way ... it is going there, but south of [geographical location] or north of [geographical location]. So we know ... help them visualize the routes of the rest of the traffic. It is a bit what [other SMA employee] and others work with, which the future should be like, that you can see these routes in your sea chart ... so we help them to visualize this with information.

Specifically, as, e.g., mixed traffic will involve different roles in interactions with the reasoning of MASSs, it would be difficult to allocate the emergency response task solely to roles working in either a long or a short time perspective. In other words, that an accident is to occur could be identified by operators working with other traffic. Fleet and traffic management were thus seen as equally likely to be called upon to act to prevent MASS accidents.

(The scenario involves a MASS that is closing in on an area with diving activity. The interviewee discussed at length that there are a lot of factors that have to be considered, for which information might not be available. He was then challenged in regard to missing information from the MASS.)

*Interviewer:* When would you start to worry if it [the MASS] just continued?

*Interviewee:* I would start to worry, in this case, because it is not very far away ... I would start to worry now. If it is within my mandate I would slow down the ship, and I would contact whoever is responsible for taking the decisions.

*Interviewer:* So, you would at least have the authority to slow down ships. Would that include dropping the anchor if you were really pressed for time?

*Interviewee:* Yes, I think that would have to be ... that it would be something that a traffic operator would be able to do, because that is something that you could have to ... some kind of emergency action to avoid accidents and there is no time to call anyone. You just have to make a decision. It should be within the possibilities for a traffic operator to just drop the anchor.

Any explanation thus needs to be *appropriately pruned based on the temporal and spatial distance to an accident*, even for roles typically working to other time pressures. Naturally, a maritime autonomy emergency response system needs to be explicit on any perceived hazard, such as a constantly decreasing distance to another vessel despite evasive actions. However, a situation in which a collision is deemed imminent should ideally only include the two vessels and any other hazards relevant to their trajectories. In a similar situation in which the MASS is not clear about the immediate risks, the explanation can instead include previous movements of both vessels, predicted trajectories, signalling between the vessels, etc.

*Interviewee 1:* It is like always, you have to filter, you do that all the time. Like the sea chart ... when I am piloting [a specific ship] I do not have all the information presented in the sea chart ... I do not have to know the names of all the islands. You can filter quite a lot.

*Interviewer:* How much would you filter?

*Interviewee 2:* It depends on whether you know the area or not.

*Interviewee 1:* Yes, and what you are doing. If you need to anchor a ship then you need to know where cables and pipes are laid out. That information is perhaps not super-important otherwise. It depends on what you are doing.

(This is followed by a short discussion on different configurations of the interface.)

*Interviewee 1:* Another example, say I am piloting a ship with a very clean interface ... Then one of my colleagues takes over and has a completely different preference. If something happens and I have to pilot the ship. Then perhaps I am stressed and then you have to understand the system very quickly ... and suddenly you need more detailed information about depths because you are piloting the ship outside the area you are usually in and know. It is like [Interviewee 2] says, you have to take an individual position on how much information you want presented ... how comfortable you are with the equipment.

*Interviewer:* So, you can be placed in a sudden, unexpected situation and some people want to prepare for that?

*Interviewee 1:* Yes.

Furthermore, the traffic patterns and behaviour of other vessels can differ greatly between countries or even regions. This will pose a risk when a ROC operator who monitors MASSs along long geographical routes intervenes. To support these operators, “critical areas” should be designated together with associated hazards. This will allow operators to reason about the interaction between local phenomena and safety-related reasoning by MASS designers.

*Interviewee:* We have internal guidelines to try to avoid ship meetings at one certain point in the [geographical area], at [geographical location]. But that is something most captains and pilots are aware of anyway, they do not want to meet there. So, they basically avoid it by themselves. But ... if, for some reason two ships would be on a ... are about to meet at [geographical location], especially if there are mist or foggy conditions then we are supposed to talk to them about it and get at least one of them to change their speed.

#### 4.1.3. Accept Uncertain Information Sources

Information sources are likely to be excluded to minimize the attack surface of MASSs. Indeed, MASSs are likely to rely on a well- and pre-defined set of information sources. As an example, information from the general public is likely to be disregarded or at least filtered. However, in an emergency a ROC operator can leverage such information to make decisions. Indeed, it might be prudent given who is likely to have access to, and be willing to share, relevant information. However, if such information is integrated into a maritime autonomy emergency response system, the system’s interface needs to be designed to not only convey that information but also the related certainty.

*Interviewee:* About this diving incident here. It becomes very important here that incidents like that *is reported in to somebody* ... you get ... the surveillance area for anyone surveying these ships becomes very, very large. For us, we are just VTS operators within a certain area, but anything could happen at anytime during any point on a ships route from A to B, and it can be outside of the VTS areas too. Someone starts a diving operation where there is no authority looking ... how would you get this information?

#### 4.2. On Methodological Choices

This subsection discusses results related to the two methodological choices previously described for how to implement a scenario-driven exploration of failures in an envisioned, future transportation system involving MASSs.

#### 4.2.1. Characterising the Context

The choice to be flexible by leaving certain parts of the maritime autonomy emergency response system design unspecified meant that the interviewees were pushed to describe what was missing in the context. Naturally, this meant that operators described what kind of information they would like the MASS to share.

*Interviewer:* You were thinking about contacting someone with a deeper technical understanding. How much of an expert are we talking about?

*Interviewee:* If it was a manned ship then you would just have called the engineering room to get a yes or no answer ... or we have this problem and we need this much time to fix it. During this time you need to reduce the load or something like that.

However, it also meant that they discussed what other sources of information they would like, rather than limiting themselves to those predefined by the authors.

*Interviewee:* Much of I do today is phone calls, as I am working in operations. Are there divers in the water? Is this restriction applicable? This could just as easily be solved using a website through which I could interact with restriction areas.

#### 4.2.2. Eliciting Multiple Explanations

The choice to “push/move forward” based on specific problems meant that operators often gave multiple possible explanations for problems and actions by entities in the scenarios. This was facilitated by the operators not being aware of the narrative of the failure, allowing them to speak freely about different possibilities.

(Interviewee removes a warning without realizing that a few components on the monitored MASS have broken down. This is followed by a short discussion on the interface.)

*Interviewer:* So the information you need is that it has decided to change its route, and it has, and that you can see?

*Interviewee:* Yes, and then I did a safety check, and it looked correct, although I noted that it did not end up at the same destination, but I think that is just a ... he could solve that by adding to the route. You can change that next time around, so you do not have to be confused about that. Rerouted ... then it is more believable. Otherwise I do not think ...

(Short discussion about other parts of the interface regarding other routes.)

*Interviewer:* If there were other ships in the passage, now there are none, but if there were and it decided to just move ahead ... what do you think would be required then?

*Interviewee:* Then ... when I checked the route there were no AIS targets there, but if there was one there then that route has had to change. That is a bit tricky, because then you would have had to monitor that ship using its camera when moving past that other ship. Then it becomes difficult. Then you have to pilot ... or at least monitor ... because the sensors would detect the other ship ...

### 5. Discussion

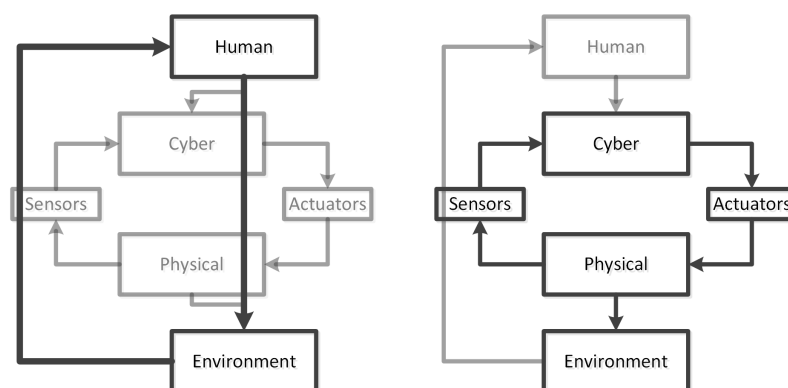
This section discusses the implications of the analysis described in the previous section, i.e., the inferences that can be made regarding the future engineering of maritime autonomy emergency response systems. It then discusses limits on these implications based on the characteristics of the study.

#### 5.1. To Design for Handling Unknown Unknowns

The contemporary engineering of critical properties for cyber–physical systems would, according to (cognitive systems) engineering ((CS)E), involve enforcing constraints on

work designs that will either allow meaningful human control or remove any reasonable likelihood of a particular accident occurring. However, for a MASS that encounters an unknown unknown any such constraints on an emergency response system involving human operators could be compromised. Referring to Endsley’s model for situational awareness [20], the results then rather point at important support that the MASS should keep running on behalf of the operator [62]: to support the operator’s comprehension of the situation, any information acquisition and analysis needs to be on par with that of a maritime domain expert; to help the operator predict the most urgent issues, the perception of elements should be kept to the minimum necessary, as defined by the closest hazard; and to help the operator perceive the elements in the situation correctly, their presence should be quantified in terms of certainty.

Firstly, this raises the question of whether the hermeneutic and embodiment man–machine relation dichotomy is sufficient when discussing an efficient emergency response for a MASS encountering an unknown unknown. If the reason for the unforeseen situation is that large parts of the MASS’ automation has broken down, then an embodiment relation should still be the goal. An emergency response system should then support operators with information as indicated in the previous paragraph, but without, e.g., burdening them with contradictory control input from the MASS. However, if most of the automation is still working as intended, then the function of human operators might rather be to provide “professionalism” [63]. In other words, operators could use their knowledge and experience to help MASSs construct and sustain an adequate response to an unpredictable and testing demand from the operational environment. In this man–machine relation it is the intelligence of the autonomous system’s cyber components that stipulates its actions, and the human operator that supports it with cues to minimize the variability of its interface to the physical system components. Figure 3 visualizes the difference in interactions essentially including the same systems, but where decisions are taken in different places.



**Figure 3.** Embodiment vs. Professionalism.

Secondly, these fundamental demands on cognition and collaboration by the maritime autonomy emergency response system have different implications due to already existing engineering guidance:

- The need to design for domain experts is supported by existing guidelines on human-centred design. These guidelines already insist on the operator being included in the design process, which should provide engineers with a path to accessing domain knowledge.
- Nor does the need to dynamically direct the attention of the ROC operators imply a need to extend the current guidance on engineering practice. Addressing this fundamental demand requires engineers to understand the capabilities of the system well, i.e., what the limitations of control in different environmental conditions are, what is an unavoidable obstacle, etc. Transferring such explicit knowledge is the aim of system and safety engineering processes.

- However, the need to accept uncertain information sources when handling unknown unknowns puts other requirements on engineering. It requires engineers to understand the cognition and motivations of more stakeholders than the ROC operator. Furthermore, these stakeholders will most likely also be operationally and managerially independent from the engineering firm's customers, i.e., the organisations operating MASSs and ROCs [64].

Referring to the last bullet point, with enough time and a well-defined context this could to some extent be captured in stakeholder-specific processes for a human-centred design. However, as the design targets unknown unknowns it will be difficult to know whether all relevant stakeholders and information sources have been considered. To at least maximize the chances that this happens, engineers must minimize the risk that they misunderstand a distant stakeholder or disregard an information source entirely. This problem rather calls for improvements to the way information is informally gathered and made understandable inside engineering firms. Typically, firms have informal, so called "gatekeepers" that provide this service in regard to external information sources [65]. With the introduction of modern information and communication technology, gatekeepers provide less pure knowledge gathering but have increased in importance as knowledge transformers [66]. Given the complexity of MASSs, the structure of the associated engineering firms are also likely to be complex. The information then has to propagate through multiple communities inside the engineering firm. Internally, so-called organisational liaisons provide the same service as gatekeepers but between communities [67]. Although less is known about this role [68], it is mostly informal and as such will rely on the work context of particular engineering disciplines. The work context of safety engineers has, for instance, been identified as leading to a specialized understanding of organisational culture that will help the understanding of how to improve organisational structures and processes [69]. Human-centred design factors for maritime autonomy are thus likely to be *engineer-centred* design factors for improving the abilities of gatekeepers and organisational liaisons.

Taken together, these two points suggest that *accountability* will become the most difficult issue to handle for engineers. As the typical handling of constraints by system engineering through requirements validation prior to product release cannot be used to guarantee safety in these situations, the engineer will be a more obvious part of each associated failure to resolve a situation safely. In situations when the ROC operator is providing professionalism to a fully functioning MASS, the level of accountability might not be high. The ROC operator might struggle to understand the automated reasoning of the MASS [61], but should otherwise be able to focus on contacting stakeholders to verify or reject information that the engineers have indicated is uncertain. However, if most of the MASS automation has broken down, at least the ROC operator attempting to remotely control the MASS will not be fully able to focus on such information handling. The correctness of and way engineers provide such information will likely have a decisive impact on whether situations can be resolved safely. This implies a dilemma for future engineering, as the situations in which engineers might be most critical in supporting ROC operators during MASS emergencies are also situations in which most of their technology is malfunctioning and their accountability is at its highest. It will likely be tempting for engineering firms to solve the situation by shutting down information services and leave the operator to handle the situation with rudimentary support.

For engineering firms to be able to take on this accountability, they must approach an engineer-centred design with the same life-cycle thinking as contemporary human-centred design focused on operators [29]. Gatekeepers and organisational liaisons also need to receive information from operations, but from a larger set of stakeholders and regarding what those stakeholders perceive as odd or even near accidents following their interactions with MASSs. This suggests that the typical system engineering processes must be supplemented with DevOps practices [70], enabling development organisations to both analyze and receive quick feedback from operations [71].



Therefore, while human-centred design might feel like a misnomer in the context of autonomous systems, it can still fill an important role. However, for the operator to have the highest chance of successfully resolving an unsafe situation involving a MASS encountering an unknown unknown, this design might have to be focused on the engineer.

### 5.2. To Make Relevant Methodological Choices

Undoubtedly it is helpful to think of new work system designs as hypotheses for an envisioned world when planning a research or engineering design study [56]. However, while this implies the need for proper hypothesis testing techniques in cases where the prototype for the work system design is emphasised, it also outlines the inherent limitations of studies with such an emphasis. Each design will take time and resources to test, and mostly offer data for narrow inferences. It is unlikely that applied researchers, or engineering firms, will have the time for an exhaustive search for an optimal solution. In fact, they might not even be capable of such a search, given that firms, e.g., can be locked into specific technological trajectories [72,73]. A well-defined work system design in the form of a prototype can easily mean that both researchers and engineers have already constrained their options for future studies. This is easily forgotten in methodological discussions regarding cognitive design.

It is then important to understand the context when conceptual design is still relatively open, i.e., to understand early, collaborative research and engineering. Processes are not well established in this part of the engineering life cycle, which means that informal, collaborative decision-making between key people in engineering communities and management can have a large impact. A work system design then not only becomes a hypothesis, but also a boundary object [74]. It makes it possible for the participants to remain partially ignorant about each others' perspectives, but at the same time anchor a tentative, common understanding. Boundary objects have to be flexible to help transfer knowledge, which explains the reason we seem to have been more successful by leaving parts of the work system design unspecified. However, this also implies another reason for why our study was successful, i.e., that the interviewees were from different research disciplines and engineering domains. Interviewees and interviewers thus complemented each other when agreeing on a common understanding. Specifically, the interviewees were knowledgeable about both safety-critical engineering and technology for constructing autonomous systems. This allowed us to bridge knowledge gaps and transfer knowledge related to the behaviour of MASSs in hazardous situations.

While it might be easy to see the need for complementing knowledge during collaborative sense-making, this particular knowledge combination might be problematic. In a firm that is attempting to be an early adopter of technology, the engineering communities are also likely to overlap in this regard [32]. However, the engineering communities at the majority of engineering firms risk being split between prioritizing understanding safety-critical engineering and novel, smart technology [32]. The majority of engineering firms might thus face larger challenges to collaboration when trying to involve enough engineers for investigating complex systems such as MASSs in hazardous situations. Similarly, cognitive design research is distinct from many of the applied research fields focusing on engineering autonomous systems. This means that the integration between communities mentioned in Section 2.3 has to be enabled, which, at least in the context of engineering organisations, would require a (cognitive) system engineering.

This also shows why our choice to favour “pushing/moving forward” on certain topics in lieu of realism was successful. The collaborative process conveyed a strong feeling of non-urgency. This meant that the interviewees favoured cognitive processes such as analytical reasoning [75], rather than those more likely at times of high task complexity and high time pressure. This was probably positive for the interview questions related to the cues for operability and acceptability. These were hypothesis-testing in the sense expected in cognitive research, and more reflection only clarified the limitations of the traffic monitoring system prototype. However, a way to explore quicker cognitive processes is to first agree about the situation in more detail, and then restart it by challenging the

interviewee through complicating his own interpretation of the situation in a way aligned with the original narrative. To exemplify, in regard to the quote in Section 4.2.2, the scenario was related to how the MASS would have trouble passing through a narrow strait due to components breaking down. The interviewee missed the broken components, and rather focused on whether there were other ships in the new strait chosen by the MASS. Therefore, the interviewer complicated this interpretation by challenging the interviewee to reason about a situation in which the MASS would have to traverse an even narrower passage. This led to further relevant explanations from the interviewee on alternative reasoning.

### 5.3. Limitations

A MASS encountering an unknown unknown can become involved in an accident without detecting that it is outside its design envelope. In this situation it would not signal an emergency. Handling this problem will most likely involve studying topics such as data analytics and diagnostics, and making associated inferences regarding engineering. This is outside the scope of this study, and the conclusions of the study might thus not cover all engineering necessary to implement well-designed maritime autonomy emergency response systems. Still, this should not have any impact on the validity of the conclusions for the engineering for the situations *inside* the scope of the study.

The study was performed within a Swedish context, with interviewees active in the maritime transportation system in Sweden. The characteristics of maritime transportation systems vary across nation states. Swedish VTSs, for instance, only provide advice, and have no legal right to order maritime vessels to take any action. However, this should primarily affect which ROC operators first become involved in MASS emergencies. In some nation states, these might be employed at privately owned ROCs providing fleet management, while in others they might come from public organisations providing VTSs. The impact on the conclusions of this study should thus be small.

The study is also not performed on engineering organisations, but rather only makes inferences regarding them. Therefore, the synthesis is by necessity not detailed in regard to engineering methods, but rather relates the discussion on design factors and methodological choices to an organisational level. The only exception is the last part of the discussion on methodological choices, which relates to cognitive processes. While we believe our reasoning in this last part of the discussion is conservative, there might be characteristics of engineering organisations or early, collaborative sense-making that make it invalid. This is a valuable research direction, which will require further research to clarify and validate.

## 6. Conclusions

A MASS can encounter unknown unknowns which make it unable to bring itself to a safe state. In this study we have, for these situations, identified fundamental demands on cognition and collaboration involving ROC operators. These demands were used to make inferences relating to both design factors and methodological choices for the future *engineering* of maritime autonomy emergency response systems.

The presence of unknown unknowns implies that human-centred design factors for maritime autonomy emergency response systems could rather be *engineer-centred*. Not in the sense that the operator should be ignored, but in the sense that engineers can also benefit from a workplace design aimed at enhancing their (human) capabilities and reducing their limitations. For engineering organisations, the inferences thus imply that engineering firms have to improve their informal gathering and sharing of information through gatekeepers and organisational liaisons. Furthermore, as the typical handling of constraints by system engineering through requirements validation prior to product release cannot be used to guarantee safety in these situations, the most difficult issue to handle for engineers will most likely be *accountability*. This implies a dilemma for future engineering, as the situations in which engineers might be most critical in supporting ROC operators during MASS emergencies are also situations in which most of their technology is malfunctioning and their accountability is at its highest. This could tempt engineering

firms to shut down information services and leave the operator to handle the most critical situations with only rudimentary support. To avoid this, engineering firms should be encouraged to develop DevOps practices, thereby increasing their ability to analyze and receive quick feedback from operations.

In regard to methodological choices, the results suggest that for the early engineering of maritime autonomy emergency response systems the typical approach of exposing relevant operators to new design concepts in scripted scenarios should include significant *flexibility* and *less focus on realism*. The *flexibility* will allow for a collaborative discussion on what would characterise the future world, as long as enough relevant expertise is brought together with the operators' understanding of the maritime domain. The work system design can thus act as a boundary object in early engineering. It is then important to note that engineering communities in organisations that are early adopters risk splitting their communities between those prioritizing the understanding of safety-critical engineering and those prioritizing the understanding of novel, smart technology. This can be an additional problem when investigating complex systems in hazardous situations. The *decreased focus on realism* will help elicit multiple explanations for problems and actions by entities in the scenarios, at least if the interviewers "push/move forward" to explore reasoning at high task complexity and high time pressure.

**Author Contributions:** Conceptualization, F.A. and P.U.; methodology, F.A. and P.U.; validation, F.A. and P.U.; investigation, F.A. and P.U.; resources, F.A.; data curation, F.A. and P.U.; writing—original draft preparation, F.A. and P.U.; writing—review and editing, F.A. and P.U.; project administration, F.A.; funding acquisition, F.A. All authors have read and agreed to the published version of the manuscript.

**Funding:** This study was supported by the Assuring Autonomy International Programme, a partnership between Lloyd's Register Foundation and the University of York.

**Informed Consent Statement:** Ethical review and approval were waived (19 April 2022) for this study by the KTH research ethics advisor at the KTH Research Support Office and the KTH's Ethics Committee (committee of the Faculty Council), who has assessed that this project does not fall under the Swedish Ethics Review Act (for further information see <https://etikprovningssystemet.se/>). Regardless, best practice in regard to research ethics were adhered to by the involved researchers, including, for instance, the obtainment of informed consent from and the thorough anonymisation of all interviewees.

**Acknowledgments:** Special thanks go to Vicki Derbyshire for her help in proofreading.

**Conflicts of Interest:** The authors declare no conflict of interest.

## Abbreviations

The following abbreviations are used in this manuscript:

AIS	Automatic Identification System
E-OCVM	European Operational Concept Validation Methodology
MASS	Maritime Autonomous Surface Ship
MDPI	Multidisciplinary Digital Publishing Institute
ROC	Remote Operations Centres
TAPI	Think-Aloud Protocol Interviewing
VTS	Vessel Traffic Service

## Appendix A. The Graphical User Interface

As mentioned in Section 3.2.2, the intent of the study was not to evaluate the graphical user interface of the reconfigured traffic monitoring system. Considerable effort was spent on trying to make sure the interviewees did not feel constrained by it. However, to give the reader an understanding of what the interviewees encountered, more information is provided in this appendix.

The graphical interface was built by configuring and extending the Carmenta TrafficWatch™ platform to meet the demands specified by the parameters and scenarios of the study. From an operator's point of view, the platform's basic configuration displays a large map where vessels, routes and obstacles are shown (see Figure A1). This map consists of sea charts provided by an online service owned by the Swedish Maritime Administration. There are also optional maps available, such as satellite images and a bathymetry layer.

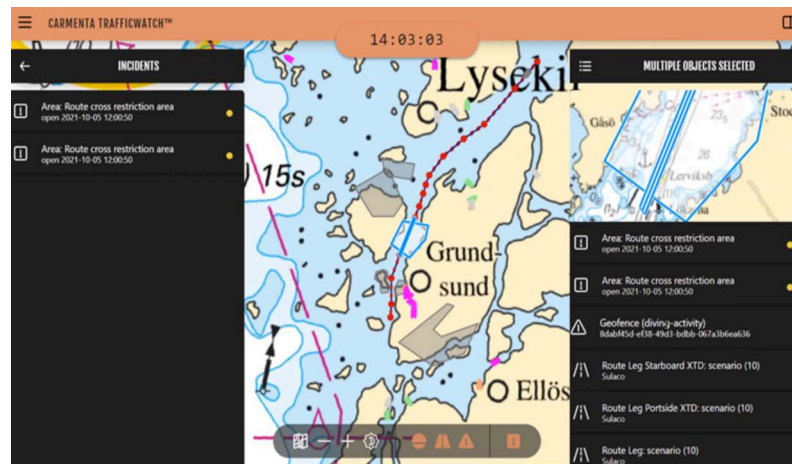


Figure A1. The Graphical User Interface.

AIS vessel positions are received from transceivers on actual ships via another online service provided by the Swedish Maritime Administration, and plotted on the sea charts. Simultaneously, simulated maritime autonomous surface vessels (MASSs) can send data directly to the platform from remote clients. In addition to standard parameters such as speed and heading, the simulated MASSs can send routes and sensor data to the platform. The sensor data may contain system health data (status indicators for navigation, propulsion, steering, etc.) and local awareness data (camera image, radar image, etc.).

Vessel routes and warnings are drawn on top of the sea charts. The latter is generated by real-time platform services that, for instance, detect when a route intersects with a restricted area. All other information is provided in panels, which can be opened to provide more information, typically by selecting an entity on the map, or closed to increase the map view. This includes panels for:

- Lists of different types of vessels.
- Lists of routes.
- Information about and from specific vessels, routes and restriction areas, including, for instance, the location of a vessel, camera images, and the purpose of a restriction area.
- A simple system health view in the form of a dynamic tree structure, color coded to indicate faults. This view was included to prompt practitioners to start talking about possible faults in MASSs and how they would like to diagnose and handle them. One example of this view is shown in Figure A2.

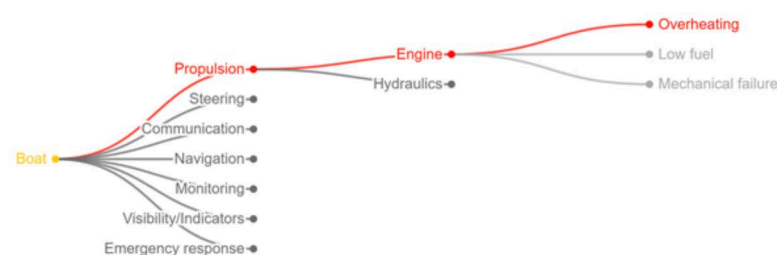


Figure A2. The Health View.

## Appendix B. The Scenarios

The scenarios were made up of different combinations of simulated maritime autonomous surface vessels (MASSs), routes, sensor data and obstacles to allow the examination of how operators would respond to both mundane and difficult situations involving MASSs and remote operations centres (ROCs). Each scenario is described below as a sequence of events, with additional information on things that were varied between different interviews.

As noted in Section 3.2.1, these scenarios were not used for testing a new work system design, but rather used to explore fundamental demands on cognition and collaboration due to failures induced by general design errors.

### *Appendix B.1. MASS Breakdown, Autonomous Rerouting*

1. MASS sends initial route to ROC.
2. MASS sends continuous position updates which can be seen by operators in real time.
3. MASS has a system health breakdown (variable breakdown). MASS updates state and sees risk on route, prompting route recalculation.
  - A health data message is sent to ROC.
  - A route update message is sent to ROC (including reason for change). This leads to the ROC operator being notified.
4. ROC looks up action to take for malfunction, which is to increase the safety margins. ROC infrastructure (also) detects that the increased safety margins and a hazard overlap and generates a notification.
  - Variability, as in different types of breakdowns affecting MASS capability differently:
    - Simple breakdown with complete loss of functionality.
    - Complex breakdown where capability is reduced rather than completely lost.
5. Operators see notifications. (Prompted by vessel and self-identified.)
6. ROC updates vessel information:
  - Route change
  - Capability reduction
7. Operators can look at notifications, MASS information, etc. (MASS and ROC situational awareness.)

### *Appendix B.2. MASS Breakdown, No Autonomous Rerouting*

1. MASS sends initial route to ROC.
2. MASS sends continuous position updates which can be seen by operators in real time.
3. MASS has a system health breakdown (variable breakdown).
  - A health data message is sent to ROC.
  - Variability, as in different types of breakdowns affecting capability differently (incident can thus be different, but here we use a grounding incident as an example): Simple breakdown with complete loss of functionality, and complex breakdown where capability is reduced rather than completely lost.
4. ROC looks up action to take for malfunction, which is to increase the safety margins. ROC infrastructure (also) detects that the increased safety margins and a hazard overlap and generates a notification.
  - Variability, as in:
    - That the restricted area could be due to different global weather phenomena not updated on MASS.
    - The MASS could have an old map (so, a health message was probably sent much earlier, but was not critical at that point in time).
5. Operators see incidents and notifications. (Prompted by vessel and self-identified.)
6. ROC updates vessel information:

- Capability reduction
7. Operators can look at notifications, MASS information, etc. (MASS and ROC situational awareness.)

#### *Appendix B.3. Multi-Malfunctions in MASS Subsystems*

1. MASS sends initial route to ROC.
2. MASS sends continuous position updates which can be seen by operators in real time.
3. MASS has a system health breakdown (engine malfunction). MASS updates state and sees risk on route, prompting route recalculation.
  - A health data message is sent to ROC.
  - A route update message is sent to ROC (including reason for change). This leads to the ROC operator being notified.
4. ROC looks up actions to take for engine malfunction; it is decided to increase the safety margins. ROC infrastructure (also) detects that the increased safety margins and a hazard overlap and generates a notification.
5. MASS has a system health breakdown (AIS malfunction). (Prompts no route change.)
  - A health data message is sent to ROC.
6. MASS has a system health breakdown. (Radar malfunction). MASS updates state and sees risk in current speed, prompting route recalculation.
  - A health data message is sent to ROC.
  - A route update message is sent to ROC (including reason for change). This leads to the ROC operator being notified.
7. Operators see incidents and notifications. (Prompted by vessel and self-identified.)
8. ROC updates vessel information:
  - Route change
  - Capability reduction
9. Operators can look at notifications, MASS information, etc. (MASS and ROC situational awareness.)

#### *Appendix B.4. Restricted Area on Route, Seen by MASS Situational Awareness*

1. MASS sends initial route to TW.
2. MASS sends continuous position updates which can be seen by operators in real time.
3. MASS sends notification of route change, including reason (which is restricted area on route).
  - Variability, as the restricted area could be due to:
    - Different local weather phenomena identifiable by MASS (e.g., fog).
    - An old map (so, a health message probably sent much earlier, but which was not critical at that point in time).
4. Operator receives notification that MASS has changed course due to restricted area on MASS route.
5. Operator investigates notification (ROC situational awareness), not seeing the restricted area.
6. Operator investigates MASS. (MASS situational awareness.)

#### *Appendix B.5. Other Ship on Collision Course with MASS, Autonomous Rerouting*

1. MASS sends initial route to ROC.
2. MASS sends continuous position updates which can be seen by operators in real time.
3. MASS sends notification of route change, including reason (which is ship on collision course).
4. Operator receives notification that MASS has changed course due to another ship being on collision course with MASS.

5. Operator investigates notification (ROC situational awareness), not seeing the ship.
6. Operator investigates MASS. (MASS situational awareness.)
  - Variability in reason for collision risk due to different ships seen on radar and camera, i.e., ferry, super-tanker, kayaks, speedboat, slow cruiser and fishing boat.
  - Information via radio from, e.g., fishing boat.

*Appendix B.6. Other Ship on Collision Course with MASS, No Autonomous Rerouting*

1. MASS sends initial route to ROC.
2. MASS sends continuous position updates which can be seen by operators in real time.
3. Operator receives notification that ship is on collision course with MASS.
4. Operator investigates notification. (ROC situational awareness.)
5. Operator check whether MASS sees same indication, which it does not. (MASS situational awareness.)

*Appendix B.7. New Route from MASS Crosses Restricted Area*

1. MASS sends initial route to ROC.
2. MASS sends continuous position updates which can be seen by operators in real time.
3. MASS notices object in route. MASS sends notification of route change, including reason (which is ship on collision course).
  - Variability in different ships detected, i.e., ferry, super-tanker, kayaks, speedboat, slow cruiser, and fishing boat.
4. ROC receives notification that MASS has changed course due to another ship being on collision course with MASS.
5. ROC receives notification that MASS route interferes with restricted areas.
6. Operator investigates notification. (ROC situational awareness.)
  - Variability in different restricted areas, i.e., dangerous, fog, restricted, etc.
7. Operator checks whether MASS sees same indication, which it does not. (MASS situational awareness.)
8. ROC checks route and sees that it interferes with restricted area. (ROC situational awareness.)

*Appendix B.8. Restricted Area on Route, Seen in ROC Situational Awareness*

1. MASS sends initial Route to ROC
2. MASS sends continuous position updates which can be seen by operators in real time
3. ROC receives alert from external system that there is a temporary restriction area along the MASS route.
4. Operator investigates notification. (ROC situational awareness.)
5. Operator checks whether MASS sees same indication, which it does not. (MASS situational awareness.)

*Appendix B.9. Several Other Ships on Collision Course with MASS*

1. MASS sends initial route to ROC.
2. MASS sends continuous position updates which can be seen by operators in real time.
3. ROC backend discovers that the route crosses an area with other vessels (it receives these objects from AIS).
4. Operator receives multiple notifications that ships are on collision course with MASS.
5. Operator investigates notification. (ROC situational awareness.)
  - Variability in reason for collision risk:
    - Planned route on wrong side of fairway.
    - Area of fog.
    - Restricted area due to drifting, burning ship on route.

6. Operator checks whether MASS sees same indication, which it does not. (MASS situational awareness.)

#### Appendix B.10. Multi-Notifications from MASS

1. Several MASSs send initial Route to ROC.
2. Several MASSs send continuous position updates which can be seen by operators in real time.
3. Weather change prompts increase of risk contours across large area with several MASSs.
4. Several MASSs send notification of route change, including reason (which is ships at risk of grounding).
5. One MASS does not, but operator receives notification that this MASS is at risk of grounding.
6. Operator investigates notifications. (ROC situational awareness.)
  - Variability in different restricted areas, i.e., dangerous, fog, restricted, etc.
7. Operator checks whether MASS (1) sees same indication, which it does not.

## References

1. Norwegian Forum for Autonomous Ships. Definitions for Autonomous Merchant Ships. Report. 2017. Available online: <https://nfas.autonomous-ship.org/wp-content/uploads/2020/09/autonom-defs.pdf> (accessed on 30 April 2022).
2. Iwanaga, S. Legal Issues Relating to the Maritime Autonomous Surface Ships' Development and Introduction to Services. Master's Thesis, World Maritime University, Malmö, Sweden, 2019.
3. Institute for Energy Technology. *Identification of Information Requirements in ROC Operations Room*; Technical Report; Institute for Energy Technology: Kjeller, Norway, 2020.
4. Fan, C.; Wróbel, K.; Montewka, J.; Gil, M.; Wan, C.; Zhang, D. A framework to identify factors influencing navigational risk for Maritime Autonomous Surface Ships. *Ocean Eng.* **2020**, *202*, 107188. [[CrossRef](#)]
5. *Outcome of the Regulatory Scoping Exercise for the Use of Maritime Autonomous Surface Ships (MASS)*; MSC. 1/Circ. 1638; International Maritime Organization: London, UK, 2021.
6. Lloyd's Register. *ShipRight, Design and Construction, Additional Design Procedures, Design Code for Unmanned Marine Systems*; Lloyd's Register Group Limited: London, UK, 2017.
7. Bainbridge, L. Ironies of automation. *Automatica* **1983**, *19*, 129–135. [[CrossRef](#)]
8. Wiener, E.L. *Human Factors of Advanced Technology ("Glass Cockpit") Transport Aircraft*; Technical Report; NASA Ames Research Center: Mountain View, CA, USA, 1989.
9. Stanton, N. Product design with people in mind. *Hum. Factors Consum. Prod.* **1998**, *1*–17.
10. *Standard ISO 21448:2022; Road Vehicles—Safety of the Intended Functionality*. International Organization for Standardization: Geneva, Switzerland, 2019.
11. Dekker, S.W.; Woods, D.D. To intervene or not to intervene: The dilemma of management by exception. *Cogn. Technol. Work.* **1999**, *1*, 86–96. [[CrossRef](#)]
12. Löscher, I.; Axelsson, A.; Vännström, J.; Jansson, A. Eliciting strategies in revolutionary design: Exploring the hypothesis of predefined strategy categories. *Theor. Issues Ergon. Sci.* **2018**, *19*, 101–117. [[CrossRef](#)]
13. Norman, D.A. Cognitive engineering. *User Centered Syst. Des.* **1986**, *31*, 61.
14. Norman, D. *Things That Make Us Smart: Defending Human Attributes in the Age of the Machine*; Addison Wesley Publishing Co.: Reading, MA, USA, 1993.
15. Ashby, W.R. *An Introduction to Cybernetics*; Chapman and Hall Ltd.: London, UK, 1956.
16. Hollnagel, E.; Woods, D.D. *Joint Cognitive Systems: Foundations of Cognitive Systems Engineering*; CRC Press: Boca Raton, FL, USA, 2005.
17. Rasmussen, J.; Pejtersen, A.M.; Goodstein, L.P. *Cognitive Systems Engineering*; Wiley: Hoboken, NJ, USA, 1994.
18. Wiener, E.L.; Curry, R.E. Flight-deck automation: Promises and problems. *Ergonomics* **1980**, *23*, 995–1011. [[CrossRef](#)]
19. Sarter, N.B.; Woods, D.D.; Billings, C.E. Automation surprises. In *Handbook of Human Factors and Ergonomics*, 2nd ed.; Wiley: Hoboken, NJ, USA, 1997; pp. 1926–1943.
20. Endsley, M.R. Toward a theory of situation awareness in dynamic systems. *Hum. Factors* **1995**, *37*, 85–104. [[CrossRef](#)]
21. Leveson, N.G. *Engineering a Safer World: Systems Thinking Applied to Safety*; The MIT Press: Cambridge, MA, USA, 2016.
22. Baxter, G.; Sommerville, I. Socio-technical systems: From design methods to systems engineering. *Interact. Comput.* **2011**, *23*, 4–17. [[CrossRef](#)]
23. Reason, J. *Managing the Risks of Organizational Accidents*; Routledge: Abingdon, UK, 2016.
24. Herbert, S. The architecture of complexity. *Proc. Am. Philos. Soc.* **1962**, *106*, 467–482.
25. Checkland, P. *Systems Thinking, Systems Practice*; John Wiley & Sons: New York, NY, USA, 1981.



26. Kelly, T. Software Certification: Where is Confidence Won and Lost? In *Addressing Systems Safety Challenges*; Anderson, T., Dale, C., Eds.; Safety Critical Systems Club: York, UK, 2014.
27. Maier, M.W. *The Art of Systems Architecting*; CRC Press: Boca Raton, FL, USA, 2000.
28. Department of Defense, Systems Management College. *Systems Engineering Fundamentals*; Technical Report; Defense Acquisition University Press: Fort Belvoir, VA, USA, 2001.
29. *Standard ISO/TS 18152:2010*; Ergonomics of Human-System Interaction—Specification for the Process Assessment of Human-System Issues. International Organization for Standardization: Geneva, Switzerland, 2010.
30. *Standard ISO/IEC/IEEE 15288:2015*; Systems and Software Engineering—System Life Cycle Processes. International Organization for Standardization: Geneva, Switzerland, 2015.
31. National Research Council. Managing Risks. In *Human-System Integration in the System Development Process: A New Look*; National Academies Press: Washington, DC, USA, 2007; Book Section 4, pp. 75–90. [[CrossRef](#)]
32. Asplund, F.; Holland, G.; Odeh, S. Conflict as software levels diversify: Tactical elimination or strategic transformation of practice? *Saf. Sci.* **2020**, *126*, 104682. [[CrossRef](#)]
33. Brown, J.S.; Duguid, P. Knowledge and organization: A social-practice perspective. *Organ. Sci.* **2001**, *12*, 198–213. [[CrossRef](#)]
34. Bolisani, E.; Scarso, E. The place of communities of practice in knowledge management studies: A critical review. *J. Knowl. Manag.* **2014**, *18*, 366–381. [[CrossRef](#)]
35. Lesser, E.L.; Storck, J. Communities of practice and organizational performance. *IBM Syst. J.* **2001**, *40*, 831–841. [[CrossRef](#)]
36. Leonard, D.; Sensiper, S. The role of tacit knowledge in group innovation. *Calif. Manag. Rev.* **1998**, *40*, 112–132. [[CrossRef](#)]
37. Asplund, F.; McDermid, J.; Oates, R.; Roberts, J. Rapid Integration of CPS Security and Safety. *IEEE Embed. Syst. Lett.* **2018**, *11*, 111–114. [[CrossRef](#)]
38. Choi, B.C.; Pak, A.W. Multidisciplinarity, interdisciplinarity and transdisciplinarity in health research, services, education and policy: 1. Definitions, objectives, and evidence of effectiveness. *Clin. Investig. Med.* **2006**, *29*, 351–364.
39. Choi, B.C.; Pak, A.W. Multidisciplinarity, interdisciplinarity, and transdisciplinarity in health research, services, education and policy: 2. Promotors, barriers, and strategies of enhancement. *Clin. Investig. Med.* **2007**, *30*, E224–E232. [[CrossRef](#)]
40. Nootboom, B. Learning by interaction: Absorptive capacity, cognitive distance and governance. *J. Manag. Gov.* **2000**, *4*, 69–92. [[CrossRef](#)]
41. Nootboom, B.; Van Haverbeke, W.; Duysters, G.; Gilsing, V.; Van den Oord, A. Optimal cognitive distance and absorptive capacity. *Res. Policy* **2007**, *36*, 1016–1034. [[CrossRef](#)]
42. Wenger, E. Communities of practice and social learning systems. *Organization* **2000**, *7*, 225–246. [[CrossRef](#)]
43. Szulanski, G. The process of knowledge transfer: A diachronic analysis of stickiness. *Organ. Behav. Hum. Decis. Process.* **2000**, *82*, 9–27. [[CrossRef](#)]
44. Rogers, E.M. Diffusion Networks. In *Diffusion of Innovations*, 4th ed.; The Free Press: New York, NY, USA, 1995; Book Section 8.
45. Nochur, K.S.; Allen, T.J. Do nominated boundary spanners become effective technological gatekeepers? (technology transfer). *IEEE Trans. Eng. Manag.* **1992**, *39*, 265–269. [[CrossRef](#)]
46. Haas, A. Crowding at the frontier: Boundary spanners, gatekeepers and knowledge brokers. *J. Knowl. Manag.* **2015**, *19*, 1029–1047. [[CrossRef](#)]
47. Rasmussen, J.; Pejtersen, A.M.; Goodstein, L.P. Work Domain Analysis. In *Cognitive Systems Engineering*; John Wiley & Sons, Inc.: New York, NY, USA, 1994; Book Section 2.
48. De Weck, O.L.; Roos, D.; Magee, C.L. From Inventions to Systems. In *Engineering Systems: Meeting Human Needs in a Complex Technological World*; MIT Press: Cambridge, MA, USA, 2011; Book Section 1, pp. 1–22.
49. Sjöfartsverket. Available online: <https://www.sjofartsverket.se/en/> (accessed on 19 March 2022).
50. Trafikverket. Available online: <https://www.trafikverket.se/en/> (accessed on 19 March 2022).
51. Färjerederiet, T. *Vision 45, Den Gula Färjan ska bli Grön*; Report; Trafikverket: Borlänge, Sweden, 2020.
52. Elwinger, T.; Ödeen, J. *Functional Specification, Operator Environment & Integrated Shipboard System*; Report; Sjöfartsverket: Norrköping, Sweden, 2020.
53. Borst, C.; Bijsterbosch, V.A.; Van Paassen, M.; Mulder, M. Ecological interface design: Supporting fault diagnosis of automated advice in a supervisory air traffic control task. *Cogn. Technol. Work* **2017**, *19*, 545–560. [[CrossRef](#)]
54. Metzger, U.; Parasuraman, R. Automation in future air traffic management: Effects of decision aid reliability on controller performance and mental workload. In *Decision Making in Aviation*; Routledge: London, UK, 2017; pp. 345–360.
55. *E-OCVM, European Operational Concept Validation Methodology*; Version 3.0, Volume I; European Organisation for the Safety of Air Navigation: Brussels, Belgium, 2010.
56. Woods, D.; Dekker, S. Anticipating the effects of technological change: A new era of dynamics for human factors. *Theor. Issues Ergon. Sci.* **2000**, *1*, 272–282. [[CrossRef](#)]
57. Quinn Patton, M. Qualitative Interviewing. In *Qualitative Research and Evaluation Methods*; Sage Publications, Inc.: London, UK, 2015; Book Section 7.
58. Brinkmann, S.; Kvale, S. Conducting an Interview. In *InterViews, Learning the Craft of Qualitative Research Interviewing*, 3rd ed.; Sage Publications, Inc.: London, UK, 2015; Book Section 7, pp. 125–147.
59. Wahl, T. Exploring a Supervisory Interface for a Fleet of Semi-Autonomous Vessels. Master's Thesis, Aalto University, Espoo, Finland, 2019.

60. Quinn Patton, M. Fieldwork Strategies and Observation Methods. In *Qualitative Research and Evaluation Methods*; Sage Publications, Inc.: London, UK, 2015; Book Section 6.
61. Glomsrud, J.A.; Ødegårdstuen, A.; Clair, A.L.S.; Smogeli, Ø. Trustworthy versus explainable AI in autonomous vessels. In Proceedings of the International Seminar on Safety and Security of Autonomous Vessels (ISSAV) and European STAMP Workshop and Conference (ESWC), Helsinki, Finland, 17–20 September 2019; pp. 37–47.
62. Parasuraman, R.; Sheridan, T.B.; Wickens, C.D. A model for types and levels of human interaction with automation. *IEEE Trans. Syst. Man -Cybern.-Part Syst. Humans* **2000**, *30*, 286–297. [[CrossRef](#)]
63. McDonald, N. Organisational Resilience and Industrial Risk. In *Resilience Engineering: Concepts and Precepts*; Ashgate: Aldershot, UK, 2006; Chapter 11, pp. 155–180.
64. Maier, M.W. Architecting principles for systems-of-systems. *Syst. Eng. J. Int. Counc. Syst. Eng.* **1998**, *1*, 267–284. [[CrossRef](#)]
65. Paul, S.; Whittam, G. Business angel syndicates: An exploratory study of gatekeepers. *Ventur. Cap.* **2010**, *12*, 241–256. [[CrossRef](#)]
66. Whelan, E.; Donnellan, B.; Golden, W. Knowledge Diffusion in Contemporary R&D Groups; Re-Examining the Role of the Technological Gatekeeper. In *Knowledge Management and Organizational Learning*; King, W.R., Ed.; Springer: Boston, MA, USA, 2009; pp. 80–93.
67. Tushman, M.L. Special boundary roles in the innovation process. *Adm. Sci. Q.* **1977**, *22*, 587–605. [[CrossRef](#)]
68. Marrone, J.A. Team boundary spanning: A multilevel review of past research and proposals for the future. *J. Manag.* **2010**, *36*, 911–940. [[CrossRef](#)]
69. Asplund, F.; Ulfvengren, P. Work functions shaping the ability to innovate: Insights from the case of the safety engineer. *Cogn. Technol. Work* **2021**, *23*, 143–159. [[CrossRef](#)]
70. Leite, L.; Rocha, C.; Kon, F.; Milojevic, D.; Meirelles, P. A survey of DevOps concepts and challenges. *ACM Comput. Surv. (CSUR)* **2019**, *52*, 1–35. [[CrossRef](#)]
71. Claps, G.G.; Svensson, R.B.; Aurum, A. On the journey to continuous deployment: Technical and social challenges along the way. *Inf. Softw. Technol.* **2015**, *57*, 21–31. [[CrossRef](#)]
72. Dosi, G. Technological paradigms and technological trajectories: A suggested interpretation of the determinants and directions of technical change. *Res. Policy* **1982**, *11*, 147–162. [[CrossRef](#)]
73. Knudsen, T.; Levinthal, D.A. Two faces of search: Alternative generation and alternative evaluation. *Organ. Sci.* **2007**, *18*, 39–54. [[CrossRef](#)]
74. Nicolini, D.; Mengis, J.; Swan, J. Understanding the role of objects in cross-disciplinary collaboration. *Organ. Sci.* **2012**, *23*, 612–629. [[CrossRef](#)]
75. Hassall, M.E.; Sanderson, P.M. A formative approach to the strategies analysis phase of cognitive work analysis. *Theor. Issues Ergon. Sci.* **2014**, *15*, 215–261. [[CrossRef](#)]