Adopting the CRIOP framework as an Interdisciplinary Risk Analysis Method in the Design of Remote Control Centre for Maritime Autonomous Systems

Åsa S. Hoem[1], Ørnulf J. Rødseth[2], Stig Ole Johnsen[3]

[1] Norwegian University of Science and Technology (NTNU), Department of Design, 7491 Trondheim, Norway
[2] SINTEF Ocean, Department of Energy and Transport, 7052 Trondheim, Norway
[3] SINTEF Digital, Department of Safety, 7052 Trondheim, Norway

Humans are increasingly asked to interact with automation in complex and large-scale systems. The International Maritime Organization (IMO) has started working on regulations for Maritime Autonomous Surface Ships (MASS). For the foreseeable future, unmanned ships will most likely be under supervision from a Remote Control Centre (RCC), called constrained autonomy. We see a need to include the end-user and carry out a risk-based design analysis, considering the operational quality of the RCC. This paper proposes an approach based on the CRIOP method, short for Crisis Intervention and Operability analysis. Could this framework be adapted to the evaluation of RCC used for MASS operations? What critical scenarios should be used for evaluations of the design/HMI of an RCC? The paper recommends Operational Envelopes to describe the constraints of the system and concludes with recommendations regarding an interdisciplinary, collaborative, and anticipatory analysis of the HMI to enhance operator performance and reliability.

Keywords: HAI, HMI, Remote Control Centre, Maritime Autonomous Systems, Risk Analysis, ConOps, Use Case, CRIOP, Scenario Analysis,

1 Introduction

On the topic of MASS, the majority of papers published to date focuses on technical aspects of the ship operations and design, indicating that most scholars focus on the high-end components of the system, while organizational and human-oriented issues remain under-explored [1]. Without changes in the regulatory framework, safe interactions between conventional ships and MASS will be a significant challenge. In the foreseeable future, it is doubtful that MASS can operate without human supervision and intervention [2]. Thus, a technology-centred approach will miss the critical human element in MASS operations. Focus on controls, software, and sensors will inevitably be of limited use if little attention is afforded to the human operators' needs in the larger system [3]. This article presents a method to facilitate risk analyses to ensure a safe and resilient design of an RCC and the human-automation interface (HAI).

2 Background

MASS could better be an abbreviation for Maritime Autonomous Ship *System*, as they are complex socio-technical systems consisting of equipment, machines, tools, technology, and a work organization. The system includes functions on the ship as well as onshore – not the least the RCC. Designing such a system should follow principals of socio-technical design, like involving the future users of the new systems. Some of the leading methods for assessing safety in complex systems (e.g. STAMP, FRAM), take the necessary systemic perspective that explores the relationships between causal factors within the systems and addresses the complexity known to be important for improving safety in modern organizations [4]. However, for novel systems like MASS, the knowledge level on detailed designs is low, and the uncertainty still high.
Consequently, it is not easy to apply such systemic safety models to support the initial design phase as they rely on detailed and high-qualitative data. Besides, the methods share a challenge of being time-consuming, resource-intensive and needing extensive expert knowledge to facilitate the analysis. In this early phase, we need a more straightforward cross-disciplinary method, including the end-user, to carry out a risk-based design analysis.

3 Risk-Based Design

According to current best practice, MASS will have to be approved according to principals for "Alternatives and Equivalents" [5], which is fundamentally a risk-based approach. In national guidelines, this is partly translated to a strong focus on the ship's intended operation that needs to be described in detail [6]. This description is part of the Concept of Operations (CONOPS) that most class societies and the Norwegian Maritime Authorities requires. Risk-based design (also known as Design for Safety) is a formalized methodology, introduced in the maritime industry as a design paradigm to help bestow safety as a design objective and not a constraint. In short, it means carrying out risk analysis and consider potential risk in the different phases of design and hence treat safety as a life cycle issue. The goal is to use the information obtained from the analysis to engineer or design out accidents before they occur. A risk-based approach is recommended by Lloyd's Register [7] and DNV [8]. Structured risk-analyses should be performed on several abstraction-levels, typically utilizing several different risk-analyzing methodologies [8]. One method is the CRIOP method, which can describe and model risk qualitatively and use best practices to ensure that human factors issues are integrated into the design.

4 CRIOP – Crisis Intervention and Operability Analysis

CRIOP is an established, standardized scenario method for Crisis Intervention and Operability analysis. The methodology was developed primarily for the oil and gas industry, back in 1990 [9]. The initial scope was a scenario-and-general-checklist method for evaluating offshore control centres (CC) focusing on the human aspects in terms of conditions for successful crisis handling. Since then, the methodology has developed through collaborations between regulatory authorities, operators, research institutions, contractors and consultants, to include/consider HMIs, best practices standards and Human Factors. Integrated operations and e-Operations are now included as remote support, or remote operations are more common, due to organizational and technical changes. Today, CRIOP is used to verify and validate an RCC's ability to handle all operational modes safely and efficiently, i.e. normal operations, maintenance, disturbance/deviations, safety-critical situations.

The key elements of CRIOP are checklists covering relevant areas in the design of a control centre, Scenario Analysis of critical scenarios and a learning arena where the operators, designers and managers can meet and evaluate the optimal control centre [9].

The CRIOP process consists of four major work tasks:

1. **Prepare and organize** by defining, gather necessary documentation, establish an analysis group, identifying relevant questions and scenarios and set a schedule.
2. **General Analysis (GA)** with checklists to verify that the CC satisfies the stated requirements based on best industry practice (a standard design review).
3. **Scenario Analysis** of critical scenarios. An experienced team of end-users should perform the analysis to validate that the control centre satisfies the actual needs.
4. **Implementation and follow up:** At the end of task 2. and 3. the findings and recommendations are documented, and an action plan is established.

The method can be applied at different phases of the lifecycle, as shown in Fig. 1 below.

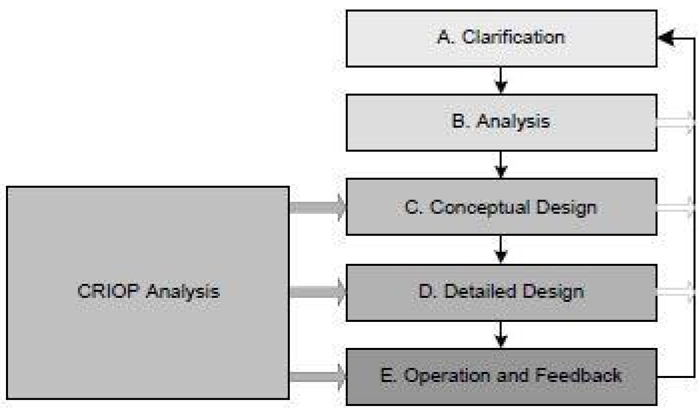

Fig. 1. Integration of CRIOP analysis in ISO 11064 design process (adapted from [9]).

This paper focuses on the methodology's applicability in the early phase, the Conceptual Design phase. Here, concepts, automation level, HMI/Alarms (displays, controls, and communication interfaces), and necessary layouts should be developed.

Results from preliminary task analysis, function allocation and job design analysis should be available before starting a CRIOP. However, RCC for MASS does not yet exist. Hence, such analyses are difficult to conduct due to the lack of established domains or users. Based on methods presented in [10], a pilot domain must be created. With a layout of a pilot domain for an RCC with operational envelopes in place, the CRIOP process can start.

We ask if the CRIOP framework could be adapted to the evaluation of RCC used for MASS operations. The general checklists must be updated, but the core ergonomics and risk-influencing factors (alarm philosophy, physical work environment, training) will be similar for an RCC for MASS and an offshore installation. Nevertheless, the risk analysis of a MASS and an offshore installation is quite different. We ask what key scenarios should be used for evaluations of the design/HMI of an RCC. Hence, we focus on the applicability of the work task 3 in the framework, the Scenario Analysis.

5 Operational envelope and use cases

The AUTOSHIP project has published an architectural concept [11], where the MASS' intended operations are broken down into smaller sets of generalized tasks, i.e. use cases. Each use case will be defined by operational constraints, e.g. geographic complexity, traffic complexity, worst-case weather, visibility conditions, etc. Together, these use cases define the MASS' Operational Envelope. This concept was first proposed in [13], calling it the operational design domain (ODD). The name was later changed to Operational Envelope to distinguish it from the ODD often used in the context of autonomous cars.

Each use case in the operational envelope describes and define both the automation's and the human's responsibilities, and the conditions that determine when responsibilities changes. [14] introduce two other important concepts, the maximum response time T_{MR}, and the response deadline T_{DL}. T_{MR} is the maximum time interval a human operator need from an alert is raised to he/she is at the control position and has gained sufficient situational awareness to take safe action. T_{DL} is defined as the minimum interval until a situation arises that the automation cannot handle. [12] introduced the idea of Constrained autonomy, which is now formally defined as a property of a sub-space of the operational envelope where the automation system at all times can calculate T_{DL}. By issuing an alert to the operator when $T_{DL} \leq T_{MR}$, one can assure that the operator will intervene in time when the automation can no longer handle a situation. The operational envelope also includes descriptions of what happens when the envelope is exceeded. The MASS must then fall back to a state that poses the least risk to life, environment, and property, so-called "Minimum Risk Condition" (MRC).

6 Remote Control Centre

As MASS are novel systems, one of the main challenges is that we have no experience from the operation or design of an RCC for MASS yet. We must base our experience from other domains such as aviation, automated road transport, or centralization of ship control done on the bridge. However, some basic principles are known:

i. Most of the time, ship operations are relatively easy to automate, e.g. transit in fair weather and non-complex traffic situations. These operations should be automated, and it is not necessary or desirable to have an operator in or on the control loop. It will be too boring for a human.
ii. More complex situations will typically develop slowly and can be identified early by the automation system, e.g. worsening weather or increasing traffic (T_{DL} is known and relatively long - on the order of half an hour).
iii. Even in a more complex situation, it should be possible to automate operations, e.g. sailing in more congested waters. Automation should, in most cases be able to handle encounters between one other ship and the MASS. However, the situation becomes more ambiguous with two or more other ships (T_{DL} is known but is shorter – on the order of minutes). The safe state could be to halt ships or reduce speed to mace the situation controllable – thus, controllability is a crucial issue.
iv. A primary driving factor for MASS is to operate many smaller ships rather than one large. Having smaller vessels increases the frequency of service, which is necessary to, e.g. transfer cargo from road to sea [12]. With crew onboard, this will not be economically feasible. There will be more than one ship to monitor from the RCC.

Based on these principals, the RCC operators will typically be in charge of several ships and not closely monitor only one ship. They will be alerted to situations that the automation cannot handle and will need to take the right action. Different types of ships and shipping operations may require other RCC configurations.

7 Review of the CRIOP Scenario Analysis

The Scenario Analysis is designed to verify that the CRO (Control Room Operator) can perform the task while considering cognitive abilities, human-system interaction and other performance shaping factors. The analysis is human-centred, focusing on the CRO's interaction with the system, including communication with other personnel. Emphasis is on how the systems support the operator's situation awareness and decision making in different situations.

The Scenario Analysis assesses the RCC's actions in response to possible scenarios. Based on the scenarios, a dynamic assessment is made of interaction between essential factors in the control room, e.g. presentation of information and time available. The methodology suggests using Sequentially Timed Events Plotting (STEP) diagrams for a graphic presentation of the scenario events. For each event, questions related to the SMoC (Simple Model of Cognition) should be asked. A checklist of performance shaping factors should also be used to ask additional questions to elaborate on answers received.

The Scenario Analysis follows four main activities:

1. Selection of a realistic scenario
2. Description of the scenario employing a STEP diagram
3. Identification of critical decisions
4. Analysis of the decisions and possible evaluation of barriers

7.1 Selection of realistic hypothetical scenarios

CRIOP recommend adapting scenarios based on incidents that have occurred and hypothetical incidents constructed by the analysis group. For MASS, when the operations are described in the operational envelope, the use cases will directly define scenarios. The challenge is to select the most critical ones and investigate if the use cases do not cover other critical scenarios in the operational envelope. One source for critical scenarios can come from hazard identification methods (e.g. HazId, HazOps, FMECA). It should consider both hazards like malfunctions of the system and hazards outside the control structure. A preliminary hazard analysis (PHA) is typically established in the general analysis of a concept design. Here, participants from different fields of expertise come together in brainstorming sessions to identify hazards and rank their impact. In the AutoFerry project, such analysis used a simple checklist-based approach and identified the most critical hazardous events to be related to the control system, communication between software and hardware components, the interaction between the ferry and recreational users of the channel and hacking and cyber-sabotage[15]. Wrobel made an assessment based on 100 ship accidents and suggested three prominent cases to be explored, i.e. groundings, collisions and fires [16].

MUNIN was the first project to develop a technical concept of a MASS back in 2015. Since then, several published papers discuss potential risks of MASS operations ([17],[18],[19]) contributing to a database of hazards and critical scenarios.

In reviews of risk analysis methods for MASS, the STAMP method [20] with STPA is recommended as it defines safety as a control problem, making it desirable for complex systems. The analysis identifies unsafe control actions and unsafe transition control actions that will lead to a hazard in a particular context and worst-case environment. These unsafe actions could also provide valuable input for scenarios.

7.1.1 Criteria for selecting scenarios

The CRIOP analysis should consider a few relevant scenarios, identified as key scenarios. In [9], the criteria for selecting these scenarios are listed. Adapted for MASS, the overall criteria should be operator involvement, hazard potential, complexity (to make sure the operators stress with peak workload) and acceptance (scenario accepted as possible by all participants).

An essential feature of MASS is the dynamic levels of autonomy that may change during a voyage depending on certain conditions. Hence the following types of human-automation interaction cases must be considered for Scenario Analysis:

1. Handover from automation to the operator. For both long and short T_{DL}.
2. Operator handling parts of the operational envelope that automation cannot handle.
3. Operator actions in the case of a fallback situation to MRC.

7.2 The STEP-model

STEP is relatively simple to understand and provides a clear picture of the course of the events to illustrate what can happen in a scenario. The graphic presentation is helpful for common ground to discuss possible hazardous events. A timeline on the horizontal axis keeps the events in order, and the connected "actors" are listed in a column. The relationship between events, what caused each of them is shown by drawing arrows to illustrate the causal links.

7.3 Identifying critical decisions

The analysis can start when the scenarios are documented. For each event involving an operator, questions are asked to identify how the systems support the operator's situation awareness and his/her ability to make decisions and execute actions. The CRIOP Handbook provides checklists with questions related to the scenarios and performance shaping factors depending on if the event relates to the operator receiving information (human-system interface) or making decisions (training, procedures and time available). The checklist helps identify potential error sources in the information systems, the operator's ability to achieve an adequate level of situation awareness, and whether sufficient information is available to allow the CRO to make decisions when required. Identified problems are called "weak points". Using the identified weak points, the Scenario Analysis's final step is to identify measures that should be taken to improve the identified weak points. Prior experiences suggest that CRIOP helps identify significant challenges between human operators and automation, as the best practice guidelines are used. Often mentioned issues are the ability to grasp the situation "at a glance", and simplifying automation steps such that the operator understands the action taken by the automation.

8 Summary

This paper presents an approach based on the CRIOP method. The framework can be adapted to the evaluation of RCC used for MASS operations. Experiences from implementing automation in other domains have found a strong need to base the development of best practices from Human Factors when there is a need for human control. CRIOP could be a risk analysis tool as we ask what can go wrong, why and how, and discuss different hazards and risks. Even though CRIOP is not based on probabilistic quantification, the participants' opinion on the scenarios is vital, contributing to a qualitative evaluation of risks. Critical scenarios for evaluations of the design/HMI should involve handover situations and fallback situations where the human operator is expected to intervene.

9 Need for further research

The next step is to test the feasibility of using an adapted version of CRIOP for hazard identification and assessment of a conceptual design of a real RCC. A case study with participants to validate the method focusing on the RCC and the HAI in a situation where the human is alerted to take control, is the HAI sufficiently well designed to satisfy T_{DL}? Furthermore, in the situations where the human operator has the responsibility for overall operations, will he/she be able to do this job at a satisfactory safety level?

Acknowledgements

This paper was published with support from the SAREPTA (Safety, autonomy, remote control and operations of industrial transport systems) project financed by the Norwegian Research Council with Grant No. 267860.

References

1. Wróbel, K., Gil, M., & Montewka, J. (2020). Identifying research directions of a remotely-controlled merchant ship by revisiting her system-theoretic safety control structure. Safety Science, 129, 104797.
2. Porathe, T. & Rødseth, Ø. J. (2019). Simplifying interactions between autonomous and conventional ships with e-Navigation. Journal of Physics: Conference Series. vol. 1357:012041 (1)
3. Veitch, E., Hynnekleiv, A., & Lützhöft, M. (2020). The Operator's Stake in Shore Control Centre Design: A Stakeholders Analysis for Autonomous Ships. London, UK, DOI: 10.3940/hf.20
4. Relling, Tore (2020). A systems perspective on maritime autonomy: The Vessel Traffic Service's contribution to safe coexistence between autonomous and conventional vessels. *Doctoral Thesis at NTNU*.
5. IMO (2013). Guidelines for the Approval of Alternatives and Equivalents as provided for in Various IMO Instruments, MSC.1/Circ.1455, 24 June 2013.
6. NMA (2020), Norwegian Maritime Authorities circular RSV 12-2020, Guidelines for automation on fully or partly unmanned vessels (In Norwegian).
7. Lloyds register (2017) Code for Unmanned Marine Systems. ShipRight: Design and Construction. Additional Design Procedures
8. DNV GL (2018). Class Guideline-Autonomous and remotely operated ships. DNVGL-0264.
9. SINTEF report (2011). CRIOP Handbook from www.criop.sintef.no
10. Rutledal, Dag (2021). Designing for the unknown: Using Structured Analysis and Design Technique (SADT) to create a pilot domain for a shore control centre for autonomous ships. Submitted to the AHFE 2021 International Conference (in review).
11. Rødseth, Ø.J. (2019). Defining ship autonomy by characteristic factors. Proceedings of the 1st International Conference on Maritime Autonomous Surface Ships. SINTEF Academic Press.
12. Rødseth Ø.J., Faivre J., Hjørungnes S.R., Andersen P., Bolbot V., Pauwelyn A.S., Wennersberg L.A.L. (2020). "AUTOSHIP deliverable D3.1: Autonomous ship design standards".
13. Rødseth, Ø.J. & Nordahl, H. (2017), Definitions for autonomous merchant ships. In Norwegian Forum for Unmanned Ships, Version (Vol. 1, pp. 2017-10).
14. Rødseth, Ø.J., Psaraftis, H.N., Krause, S., Raakjær, J. and Coelho, N.F., (2020b). AEGIS: Advanced, efficient and green intermodal systems. In IOP: Materials Science and Engineering.
15. Thieme, C. A., Guo, C., Utne, I. B., & Haugen, S. (2019). Preliminary hazard analysis of a small harbor passenger ferry–results, challenges and further work. In Journal of Physics: Conference Series (Vol. 1357, No. 1, p. 012024). IOP Publishing.
16. Wróbel, K., Montewka, J., & Kujala (2017). Towards the assessment of potential impact of unmanned vessels on maritime transportation safety, *Reliability Engineering & System Safety*, *165*, 155-169.
17. Bureau Veritas (2019). NI641 guidelines for autonomous shipping.
18. Chaal, M., Banda, O. V., Basnet, S., Hirdaris, S., & Kujala, P. (2020). An initial hierarchical systems structure for systemic hazard analysis of autonomous ships. In Proceedings of the International Seminar on Safety and Security of Autonomous Vessels (ISSAV). Sciendo.
19. Fan, C., Wróbel, K., Montewka, J., Gil, M., Wan, C., & Zhang, D. (2020). A framework to identify factors influencing navigational risk for Maritime Autonomous Surface Ships. Ocean Engineering, 202, 107188.
20. Leveson, N. G. (2016). Engineering a safer world: Systems thinking applied to safety (p. 560). The MIT Press.