

Socio-Technical Considerations for the Maritime Autonomous Infrastructure

Bernard Joseph Twomey

PhD

University of York

Computer Science

June 2025

Abstract

Conventional ships benefit from a long-established framework of prescriptive regulations, classification rules, and national legislation that support consistent evaluation and certification of design, construction, and operation. However, the introduction of autonomous functions presents fundamentally different challenges. In particular, the Maritime Autonomous Infrastructure (MAI) presents a complex socio-technical system and unprecedented regulatory and operational challenges due to its distributed, cross jurisdictional nature and reliance on emerging technologies. Addressing these challenges requires a shift away from rule-based compliance to a structured assurance/safety case approach that consider all elements of the MAI, accounts for the entire lifecycle and changing operational context.

This research argues that the risks associated with the MAI differ significantly from those encountered in conventional maritime operations, particularly in the context of remotely operating or autonomous control of crewless vessel functions. These differences are amplified by the emergence of novel interdependencies within a system of systems context. Consequently, hazard identification must extend beyond the initial design phase and be maintained as a continuous, iterative process throughout the entire system lifecycle, encompassing normal operations, reasonably foreseeable abnormal events, and emergency conditions.

A key contribution of this thesis is the development of the Lifecycle Process Model (LPM), supported by the Safety Process Model (SPM), Layers of Protection (LoP) and the Maritime Autonomous Infrastructure – Design Envelope (MAI-DE). Together, these models form a coherent assurance framework tailored to the unique challenges of maritime autonomy and remotely controlled functions. Their application enables the structured identification and management of risk, facilitates cross-stakeholder engagement, and supports the development of a defensible and compelling body of evidence for demonstrating that the MAI is ‘Acceptably Safe’.

Acknowledgements

I am deeply grateful to my supervisor Professor John McDermid whose exceptional guidance, unwavering support, and intellectual generosity has been fundamental to the completion of this thesis. His ability to challenge my thinking, offer clarity amidst complexity, and encourage independent thought, have shaped the direction of this research. I have benefited greatly from the experience and consider myself fortunate to have him as my supervisor.

I would also like to thank Dr Mark Nicholson for his practical insights and grounding on what can be achieved within the available timeframe, hopefully, I did not 'Boil the Ocean'. My sincere thanks also go to the team at the Centre for Assuring Autonomy (CfAA) in the University of York, who all treated me with respect, Chryste you are amazing - thank you.

I would also like to extend my sincere thanks to friends and trusted experts who supported me and provided critical evaluation of my work throughout this process: Dr Claire Pekcan, Dr Robert Oates, Dr Anita Teo, Dr Jonathan Earthy, Dr Marin Guthrie, Erik Tvedt, Gavin Gunny and Brandon Larson – your insights and encouragement have been invaluable.

Finally, I would like to thank my family for the support and time you have given me to complete this work.

Declaration

I declare that this thesis is a presentation of original work, and I am the sole author. This work has not previously been presented for a degree or other qualification at this University or elsewhere. All sources are acknowledged as references.

Contents

CHAPTER 1 : INTRODUCTION	9
1.1 PROBLEM SPACE	9
1.2 THESIS AIMS AND KEY CONTRIBUTIONS	10
1.3 EXTERNAL DISSEMINATION AND EARLY VALIDATION.	16
CHAPTER 2 : LITERATURE SURVEY	17
2.1 INTRODUCTION.....	17
2.2 WHAT IS A CONVENTIONAL SHIP?	20
2.3 CURRENT REGULATORY DEVELOPMENTS	21
2.3.1 IMO - Non-Mandatory MASS Code.	23
2.3.2 Demonstrating Feasibility.....	24
2.4 CURRENT CLASSIFICATION SOCIETY DEVELOPMENTS.	27
2.5 AUTONOMY IN OTHER TRANSPORTATION DOMAINS.....	31
2.6 ACADEMIC STATE OF THE ART RESEARCH	35
2.6.1 Applicability of cross-sector assurance frameworks.	38
2.6.2 Future Academic Research Directions and Responsibility Gap.....	39
2.7 LITERATURE SURVEY CONCLUSION	41
2.7.1 Beyond the State of the Art and Identified Gaps.....	43
CHAPTER 3 : EVOLVING SAFETY PARADIGMS.....	45
3.1 WHAT IS A MARITIME AUTONOMOUS INFRASTRUCTURE (MAI).	45
3.1.1 MAI Unique Risks.....	46
3.1.2 Concept of ‘Acceptably Safe’.	52
3.2 SUMMARY AND TRANSITION TO THE MAI LIFECYCLE PROCESS (LPM).	54
CHAPTER 4 : MAI LIFECYCLE PROCESS MODEL (LPM).	56
4.1 RATIONALE FOR DEVELOPING THE LPM.....	57
4.2 OPERATIONAL CYCLE: CONTRASTING CONVENTIONAL AND AUTONOMOUS OPERATIONS.....	57
4.3 DEVELOPMENT AND STRUCTURE OF THE LPM	60
4.4 INTEGRATION WITH SUPPORTING MODELS.....	61
4.5 SIGNIFICANCE AND CONTRIBUTION OF THE LPM.....	61
4.6 TRANSITION TO CHAPTER 5	62
CHAPTER 5 : MAI LIFECYCLE PROCESS MODEL (LPM).	63
5.1 CONTROLLING BIAS	65
5.2 ELEMENTS OF THE LPM EXPLAINED.....	70
5.2.1 Goal	70
5.2.2 Concept.....	71
5.2.3 Voyage Plan.....	82
5.2.4 Stakeholder and Actor Analysis.....	84

5.2.5	Voyage Conditions.....	91
5.2.6	Operational Conditions.....	93
5.2.7	Hazard and Risk Analysis.....	94
5.2.8	Overall Safety Requirement.....	98
5.2.9	Fallback State	117
5.2.10	Other Risk Reduction Methods.....	118
5.2.11	Overall Safety Requirements Specification	119
5.2.12	Overall Safety Validation Planning.....	119
5.2.13	Operate Maintain Diagnose and Repair (OMDR).....	122
5.2.14	System Disposal and Transition Management in the MAI Lifecycle.	123
5.2.15	Summary	125
CHAPTER 6 : APPLICATION OF THE LPM.		127
6.1	CASE STUDIES.....	127
6.1.1	Use Case 1: Operation of Navigation Lights.....	129
6.1.2	Use Case 2: Anchoring.	136
6.1.3	Use Case 3: Emergency Condition Fire within a land-based ROC.	141
6.1.4	Use Case 4: Loss of Situational Awareness.	147
6.1.5	Key findings from the use cases.	151
6.1.6	Effectiveness and Gaps in the Lifecycle Process Model.	155
6.1.7	Evaluation of the research objectives.	157
CHAPTER 7 : BARRIERS AND CHALLENGES.		160
7.1	TRANSITIONING FROM STATIC TO DYNAMIC ASSURANCE MODELS FOR THE MAI	162
CHAPTER 8 : EVALUATION, FUTURE WORK AND CONCLUSIONS.		167
8.1	INDEPENDENT EVALUATION.....	167
8.2	FUTURE WORK: LEGAL AND REGULATORY CHALLENGES: THE ROAD AHEAD	171
8.2.1	Regulatory Change as a Dynamic Constraint	171
8.2.2	Business Risk and Economic Justification	172
8.2.3	Human-Centred Design	173
8.2.4	Intangible assets and the prospect of self-certification of the MAI	173
8.2.5	Legal and Regulatory Challenges for the MAI	175
8.2.6	Evaluation of Validity and Adoptability of the Thesis.....	176
8.2.7	Conclusions	178
CHAPTER 9 : BIBLIOGRAPHY.		180
CHAPTER 10 : APPENDIX A.....		187

List of Figures

Figure 3-1 Conceptual elements of the Maritime Autonomous Infrastructure.....	46
Figure 5-1: Lifecycle Process Model (LPM) for the MAI	67
Figure 5-2: Interdependencies between the stages of the LPM	69
Figure 5-3: Inherently Safe Design and Fault Tolerant Assessment Model	82
Figure 5-4: Safety Process Model (SPM) for the MAI.....	101
Figure 5-5: MAI Design Envelope	110
Figure 5-6: Level 1- Prevention of deviations from normal operations	112
Figure 5-7: Level 2 - Detecting and controlling deviations.....	113
Figure 5-8: Level 3 - Activation of engineered safety features	114
Figure 5-9: Limiting consequences and preventing escalation	115
Figure 5-10: Emergency response and external intervention.....	116
Figure 6-11: Arrangement of Navigation Lights	130
Figure 6-12: Operation of Navigation Lights Stage gate review.....	134
Figure 6-13: Anchoring and Mooring equipment Images courtesy of McGregor and Bulutlu marine.....	136
Figure 6-14: Emergency Condition -Fire within a land-based ROC – concept phase review ...	144
Figure 6-15: Emergency Condition -Fire within a land-based ROC - LoP	144
Figure 6-16: Stage gate review – loss of situational awareness.....	149
Figure 6-17: Anchoring Stage Gate review.....	152

List of Tables

Table 5-1: Adaption of the ONR Safety Principles for application to the MAI	75
Table 5-2: Inherently Safe Design and Fault Tolerant Design examples for Crewed and Crewless operations.....	80
Table 5-3: Comparison of stakeholders involved in remote control or autonomous operation of the MAI	90
Table 5-4: Layer of Protection Model for the MAI (LoP)	106
Table 5-5: Level 1 Scenarios	111
Table 5-6: Level 2 Scenarios	112
Table 5-7: Level 3 Scenarios	113
Table 5-8: Level 4 Scenarios	114
Table 5-9: Level 5 Scenarios	115
Table 6-1: Operation of Navigation Lights.....	133
Table 6-2: Anchoring Operations	139
Table 7-1: Barriers - Challenges and Mitigations in acceptance of the MAI	166
Table 8-1: Overview of anonymised reviewers and professional backgrounds.	167

List of Publications by the Candidate

Conference publications:

- Daniels, D., Hobbs, C., McDermid, J. A., Parsons, M. S. & Twomey, B., "Could the Introduction of Assured Autonomy Change Accident Outcomes?" Safer Systems: The Next 30 Years, Proceedings of the 30th Safety-Critical Systems Symposium. Safety Critical Systems Club, Vol. 170. p. 229-264 2022.
- B. Twomey, "Autonomy, A Vision or Reality," Royal Institute of Naval Architects, WARSHIP 2025, International conference, Glasgow.
- Edmundson A, Twomey B. "Systems Engineering – The Hard Way" - Conference: 14th International - Naval Engineering Conference and Exhibition October 2018 DOI:10.24868/issn.2515-818X.2018.009

Other publications:

- Zoe Porter, Philippa Ryan, Phillip Morgan, Joanna Al-Qaddoumi, Bernard Twomey, John McDermid, Ibrahim Habli, "Unravelling Responsibility for AI," arXiv preprint, arXiv:2308.02608, 2023.
- Balbot, V., Theotokakis, G., McCloskey, J., Vassalos, D., Boulougouris, E., Twomey, B., "A methodology to defining risk matrices – Application to inland water ways autonomous ships. Society of Naval Architects of Korea. 2022.
- Twomey, B., "System Design and Integration", "The Cyber -Enabled Ship: - What are the risks and what are the mitigations", and "System Design and Integration". Encyclopedia of Maritime and Offshore Engineering. Wiley ISBN 9781118476352: 2018.

Chapter 1 : Introduction

1.1 Problem Space

This research addresses the requirement for a structured assurance/safety process to be applied to the Maritime Autonomous Infrastructure (MAI), taking into consideration the dynamic operating conditions of the vessel functions when operating autonomously or being remotely controlled. To contextualise the research, it was essential to first understand the maritime domain, including the implications of introducing technologies that enable remote control or autonomous operations of a vessel's functions, with or without crew on board. This thesis examines the adaptations required within the maritime sector to accommodate such a fundamental change in vessel operations.

The long development phase in the production of a mandatory Maritime Autonomous Surface Ships (MASS) Code, and the absence of a globally accepted set of requirements, has necessitated extensive engagement with individual national regulators for vessel developers/operators to ensure compliance with local requirements. This reliance on national frameworks can lead to regulatory divergence among authorities, complicating certification processes, potentially slowing down industry adoption, and introducing uncertainties when arguing safety of the Maritime Autonomous Infrastructure (MAI), across different jurisdictions. To address these challenges, this thesis introduces a new conceptual framework called the MAI, defined as follows:-

The 'Maritime Autonomous Infrastructure (MAI)' is a comprehensive and multifaceted socio-technical set of elements consisting of physical, digital and tangible assets that support the safe operation of autonomous or remotely controlled functions of a vessel.

Additionally, the maritime industry lacks a comprehensive body of best practice for operating crewless vessels. With minimal historical data and very few practicable examples, developing best practice requires a combination of theoretical analysis and experimental validation. This necessitates a forward-looking approach, anticipating potential issues and proactively developing solutions.

Various claims have been made regarding the benefits of incorporating autonomous functions in the maritime sector. These include reducing the human contribution to system hazards, enhancing safety, improving efficiency through optimised ship design, and lowering operating costs by reducing onboard crew. However, there is limited empirical evidence to support these claims.

While it is undeniable that an autonomous or remotely operated ship with no crew onboard eliminates the risk of harm to seafarers, the broader claim that autonomy will **'enhance safety'** remains unverified. This issue is further compounded by the absence of a clearly defined framework for acceptable **'levels of safety'** within the IMO regulatory instruments, making such claims difficult to substantiate.

1.2 Thesis Aims and Key Contributions

This thesis aims to develop a systematic approach for identifying elements of the MAI that are critical to safety in the operation of crewless vessels employing remotely controlled or autonomous functions. This objective is realised through the **'development and application'** of a structured Lifecycle Process Model (LPM) which facilitates the identification of potential hazards within a dynamic, multi-domain, environment. To the best of the author's knowledge, no existing framework – whether the Lifecycle Process Model (LPM - Figure 5-1), Safety Process Model (SPM - Figure 5-4), Layers of Protection (LoP - Table 5-4) or the MAI - Design Envelope (MAI – DE - Figure 5-5) exists that considers all elements of the MAI in a system-of-systems (SoS) context. In addressing this gap, this thesis offers a novel contribution by proposing a coherent assurance methodology that not only supports the concept of 'Acceptably Safe' (as defined in Section 3.2.2), while also providing a basis for stakeholder engagement, regulatory evaluation, and long-term assurance across the MAI lifecycle.

The thesis aims are supported by:

- A critical review of the existing regulatory frameworks governing the maritime sector, alongside an examination of the literature relevant to the enhancement of maritime autonomy.
- The development of a LPM, SPM, and LoP to systematically identify and evaluate the hazards and risks associated with the MAI.
- The development of a MAI-DE, that implicitly links concept requirements to voyage conditions while incorporating layers of protection principles.
- Analysing potential changes within the assurance/safety requirements, when transitioning between different operational conditions.
- Providing a systematic approach to analysing autonomous and/or remotely controlled functions using the LPM process which will support the claim of 'Acceptably Safe', and the development of the compelling body of evidence suitable for submission to regulatory bodies for regulatory review.

This research does not examine the business case or legal implications of the MAI, as these areas are anticipated to be addressed through separate research efforts or future legal instruments, developed by the IMO and other relevant national authorities. Nonetheless, it is acknowledged that both the legal framework and business requirements can significantly influence the design, operation, maintenance and disposal of the MAI.

The aims defined in this thesis have been shaped by the challenges and limitations defined within the problem space and are intended to provide a structured process to address the assurance/safety needs of the MAI within a complex and evolving technological, regulatory and operational environment, along with shifting stakeholder requirements.

This research has identified four primary aspects to structure the investigation of the Maritime Autonomous Infrastructure (MAI).

- **Hazard And Safety Assessment Process:**

Building upon classical safety principles and the definition of the MAI, this research develops a comprehensive process for identifying hazards and analysing the safety of the MAI, viewed as a System of Systems (SoS)¹ [1]. This process will address hazards arising from interactions between the elements of the SoS and from the allocation of functions within the system. It considers safety under normal and reasonably foreseeable abnormal event (RFAE)² [2] conditions could impact the safety or operation of the MAI, potentially leading to an emergency³ condition.

- **Systems Design and Risk Informed Reasoning:**

The proposed safety process is supported by analysis patterns that adopt a SoS approach to design and operation of the MAI. These patterns enable structured reasoning about failure modes, risk propagation, and operational dependencies across the distributed elements of the MAI. As an example, addressing a requirement that no single point of failure leads to an intolerable risk, may reveal that a single propulsion arrangement with one shaft-line may not meet the defined requirements, thereby informing necessary design changes. However, depending on the operational context and stakeholder requirements, the loss of propulsion might be deemed an acceptable risk.

¹ **System of Systems (SoS)**—Set of systems or system elements that interact to provide a unique capability that none of the constituent systems can accomplish on its own. Note: Systems elements can be necessary to facilitate the interaction of the constituent systems in the system of systems.

² **Reasonably Foreseeable Abnormal Event (RFAE)** is an event or failure that has happened or could happen again, and is planned for.

³ **'Emergency'** : an event or situation which threatens serious damage to human welfare or threatens serious damage to the environment. adapted from the UK Civil Contingencies Act 2004 [3]

- **Safety Argumentation Approach:**

A review of the current safety argumentation processes within the maritime sector was conducted to assess their adequacy in identifying the risks associated with MAI, and in supporting informed decisions on system suitability. The research includes the development of argumentation strategies and patterns for demonstrating the safety of a maritime SoS. These arguments will be specific to a particular operational context (Use Case), and an '*argument in principle*' will be developed that can be adapted to varying legal jurisdictions.

- **Validation and Acceptance:**

The core technical work has been validated by review from leading technical and academic experts, as detailed in Chapter 8 of this thesis. This validation was complemented by the application of the developed approach to a demonstration 'Use Case' based on a real shipbuilding project. This process includes exploring variations in argument patterns to support compliance with local regulations. It also entailed presenting alternative solutions for demonstrating that the MAI is 'Acceptably Safe' to operate within a defined context of use. While validation efforts also aim to influence international regulations, these activities are beyond the scope of this thesis.

This structured approach, combining hazard analysis, system design, safety argumentation, and validation, provides a comprehensive framework for addressing the complexities of MAI safety dealt with as a SoS. The research focusses on defining and demonstrating a coherent and scalable approach to the development of an assurance/safety framework that accommodates the unique challenges and risks associated with autonomous and remotely operated maritime systems.

Chapter 2: presents a literature review of the historical, regulatory, industrial and academic landscape relevant to the Maritime Autonomous Infrastructure (MAI). It identifies a persistent reliance on crew presence in maritime safety frameworks and highlights the fragmented and inconsistent approaches proposed by the regulatory and classification societies for acceptance of remotely controlled or autonomous operations. The chapter reviews recent pilot projects and national regulatory initiatives, illustrating both technical feasibility and the challenges of harmonisation.

Academic literature is critically assessed, revealing a gap in system-level, context-sensitive analysis and approaches that integrate the dynamic, cross-domain nature of the MAI and its evolving operational context, as well as emerging concerns around responsibility and liability.

Finally, a comparative analysis with other transport domains highlights the unique operational, environmental, and assurance challenges faced by the maritime sector, particularly the need for infrastructure dependencies. The chapter concludes by identifying the need for standardisation, cross-sector learning, and future research directions, and introduces the thesis's own frameworks as a response to these gaps.

Chapter 3: examines the key challenges and characteristics of the maritime domain that provide essential context for this research.

The unique contribution of this thesis commences from **Chapter 4**, which includes the development of the Lifecycle Process Model (LPM), the Safety Process Model (SPM), Layers of Protection Model (LoP) and the MAI Design Envelope (MAI-DE), for the MAI.

Chapter 5: presents an analysis of the individual elements of the LPM, and their integration within a System of Systems (SoS) framework. It further defines the structural requirements for constructing a defensible safety assurance argument and introduces a structured methodology to support the claim of 'Acceptably Safe' and to enable the development of the compelling body of evidence suitable for submission to the regulatory bodies for regulatory review.

Chapter 6: applies, tests, and evaluates the integrated models developed in previous chapters—namely the Lifecycle Process Model (LPM), Safety Process Model (SPM), Layers of Protection (LoP), and the MAI Design Envelope (MAI-DE), through a series of representative use cases. These case studies encompass both crewed and uncrewed maritime operations, including remote and autonomous functions, and address scenarios such as navigation light operation, anchoring, abandonment of a land-based Remote Operations Centre (ROC), and loss of situational awareness. The chapter demonstrates how these models support structured risk identification, assurance development, and system integration within the Maritime Autonomous Infrastructure (MAI). It also critically evaluates the effectiveness of the models, identifying key gaps and challenges, such as the validation of fallback states, communication resilience, regulatory harmonisation, and evidence

ownership, that must be addressed to ensure robust, lifecycle-based assurance and stakeholder confidence in the safe deployment of the MAI.

Chapter 7: This chapter aims to critically examine the broader systemic, regulatory, institutional, and cultural challenges that impede the acceptance and operational deployment of the MAI. While earlier chapters focused on the technical frameworks and safety methodologies required to establish the MAI as 'Acceptably Safe,' this chapter reframes the problem by addressing the contextual conditions under which acceptance must be negotiated. It argues that technical adequacy alone is insufficient without parallel efforts to overcome regulatory fragmentation, institutional inertia, and a pervasive misunderstanding of the MAI as merely a vessel-based solution, rather than a dynamic, system-of-systems (SoS) infrastructure. Through this analysis, the chapter highlights the importance of regulatory reform, stakeholder alignment, and the development of new governance and assurance models that reflect the distributed, evolving nature of the MAI that requires infrastructure level thinking within international maritime policy and safety practices.

Finally, **Chapter 8** presents thesis findings and outlines the broader implications of the research. It begins with an independent evaluation of the proposed frameworks by a panel of external specialists, whose multidisciplinary expertise is applied to assess the completeness, applicability, and rigour of the models developed, as well as to identify areas for further development. This is followed by a discussion of priority areas for future work, including the need to adapt to evolving regulatory expectations, integrate economic and business risk considerations, and systematically embed human-centred design principles across the MAI lifecycle. The chapter concludes by reaffirming the thesis's original contribution: the development of a structured, system-of-systems approach to the safety assurance of Maritime Autonomous Infrastructure (MAI), and its potential to inform policy, practice, and future research.

1.3 External dissemination and early validation.

To assess relevance and current applicability, extracts of the proposed frameworks (MAI, LPM, SPM, LoP, MAI-DE) were presented at the RINA Warship 2025 Conference in Glasgow [129]. The presentation introduced the MAI and the associated assurance models. Audience engagement centred on scalability and domain transfer. Delegates asked whether the LPM scales across vessel types and whether the models apply to naval platforms operating under military exemptions. The responses, subsequently reviewed with subject-matter experts, clarified two main points:

- (i) the LPM is modular and stage-based, permitting tailoring to differing system complexities and mission profiles, and
- (ii) while naval vessels may operate under statutory exemptions, the frameworks are designed to demonstrate an 'Acceptably Safe' level for non-combat operations consistent with the **'at least as good as statute'** principle. A summary of questions and responses is provided in Appendix A.

In addition to academic and regulatory evaluations, industry practitioner feedback was obtained from GE Marine Engine Services, who reported on initial application of the LPM to identify risk interfaces and inform shipyard planning, thereby reducing sources of construction delay and protecting original equipment manufacturer (OEM) milestones. This feedback provides practice-based corroboration that the lifecycle approach is transferable beyond the thesis use cases; the full statement is reproduced in Appendix A with permission. These activities serve as early external validation of the frameworks' clarity, scalability, and practical utility, and they inform the evaluation reported in Chapter 8.

Chapter 2 : Literature Survey

2.1 Introduction

This chapter presents a structured literature survey, identifying and evaluating existing academic and industry work relevant to the Maritime Autonomous Infrastructure (MAI). The objective is to establish the current state-of-the-art regarding the conceptualisation, development, and the assurance/safety processes required to demonstrate that the MAI is 'Acceptably Safe' to operate in a defined context of use. Through historical, regulatory, and cross-domain analysis, this survey highlights areas of consensus and divergence, and identifies critical gaps that form the basis for the thesis's subsequent research and contributions.

The historical trajectory of maritime safety regulation is marked by persistent fragmentation and jurisdictional complexity, with regulatory requirements often varying significantly between flag states and port states. Regulatory variations have existed since the earliest codifications, such as the Venetian load line of 1255 where seafaring societies marked the sides of their ships with the predecessor of the 'load line', making it illegal to exceed the identified draught, and later the British Merchant Shipping Act of 1894 [4][5]. These inconsistencies frequently resulted in operational inefficiencies and legal ambiguities for ship operators navigating international waters. Vessels were routinely subject to overlapping, and at times contradictory safety standards, complicating compliance and undermining the predictability of certification processes. For example, individual states imposed their own conditions for the control of ships in its ports. The UK Merchant Shipping Act 1906 [6] officially applied loading and minimum load line requirements to foreign ships while the United States Seamen's Act of March 1915 [7] applied U.S. authority over foreign vessels sailing from American ports thereby overruling the requirements of the flag-state of the vessel.

This range of provisions resulted in considerable legal uncertainty, as navigational permits and seaworthiness certificates lacked international validity. Confusion reigned, to the extent that ships visiting ports in different states were sometimes required to meet contradictory safety conditions. An analysis of maritime law codes between 1255 to 1276, presented in [8] 'Conflicts in 13th Century Maritime Law: A Comparison between five European Ports' concluded that:

'the rules to be analysed are evidently the result of negotiations conducted by the parties involved: that is to say regulations on which the professional merchants and seafarers had agreed upon amongst themselves'

This highlights the long-standing reliance on decentralised, practice-based rulemaking in the maritime domain, an issue that continues to present challenges for the standardisation of autonomous vessel operations under the MAI.

The regulatory progression is reflected in the Carriage of Goods at Sea Act (Hague Rules as amended) incorporated into English law by the Carriage of Goods at Sea act 1971 [9]. This requires the carrier to exercise due diligence to make the ship seaworthy before and at the start of the voyage. The scope of this obligation was further extended by the United Nations Convention for the International Carrying of Goods wholly or partly by sea (the Rotterdam Rules) which was adopted by the United Nations on 11th December 2008, and which requires vessels to be 'seaworthy' throughout the voyage by sea.

The concept of 'Seaworthy' is a very broad and not only includes the physical state of the vessel but includes other aspects such as crewing and responsibilities of the Master as defined in the International Safety Management (ISM) Code which was adopted in 1993 by resolution A.741(18) and was made mandatory with entry into force on 1st July 1998 [10].

As defined by the Marine Insurance Act (MIA)S39:

"A ship is deemed to be seaworthy when she is reasonably fit in all respects to encounter the ordinary perils of the seas of the adventure insured". [11]

In addition, the Hague Visby Rules [12] provide that:

“ the carrier shall be bound before and at the end of a voyage to exercise due diligence to :-

(a) make a ship seaworthy and

(b) properly man, equip and supply the ship.? “

A core assumption underpinning existing maritime regulations is the continuous presence of the master and crew, whose oversight forms the basis of traditional safety assurance. Consequently, legal concepts such as 'Seaworthiness' have historically relied on human intervention, both onboard and ashore.

The preceding discussion illustrates that the maritime sector possesses a long-standing and well-developed framework for regulating vessel safety. Additionally, they emphasise the necessity for collaboration between the various stakeholders, along with the requirements for a vessel to be seaworthy as defined by the marine insurers.

As the maritime sector transitions toward the deployment of autonomous and remotely controlled vessels, these historical lessons acquire renewed relevance. The absence of harmonised international standards for Maritime Autonomous Infrastructure (MAI) risks replicating the regulatory fragmentation of the past, potentially impeding global adoption and eroding stakeholder confidence in the safety and reliability of autonomous operations. In particular, the distributed and cross-jurisdictional nature of MAI introduces unprecedented challenges for assurance, certification, and regulatory oversight, necessitating a departure from prescriptive, vessel-centric frameworks toward adaptive, goal-based methodologies.

The next section examines the state-of-the-art and beyond state-of-the-art developments within the maritime sector to address the specific challenges associated with the introduction of technologies that enable the operation of crewless, autonomous, or remotely controlled vessel functions.

2.2 What is a Conventional Ship?

The term "Conventional Ship" is not explicitly defined within the statutory instruments of the IMO. However, in the absence of a formal definition, it is widely interpreted to describe vessels that are designed and operated according to established maritime norms and regulatory requirements, including adherence to prescriptive technical requirements issued by classification societies and regulatory authority requirements to ensure that identified risks are mitigated to an acceptable level.

Vessels under the remit of the IMO are subject to the provisions of the International Convention for the Safety of Life at Sea (SOLAS) [67], which defines minimum regulations for the construction, equipment, and operation of ships. These regulations include, but are not limited to vessel stability, machinery, electrical installations, fire protection, and lifesaving appliances.

As stated by the IMO:

“The main objective of the SOLAS Convention is to specify minimum standards for the construction, equipment and operation of ships, compatible with their safety”.

At present, SOLAS and related conventions do not address the use of remote control, autonomous functions, or the operation of vessels without crew on board. This regulatory gap presents a fundamental challenge to the adoption of such vessels, as emerging technologies extend beyond the scope of traditional vessel design, operation and assurance frameworks.

Further complexity is introduced by the United Nations Convention on the Law of the Sea (UNCLOS) which uses the terms “ships and vessels” interchangeably without providing formal definition. For the purposes of this thesis, the definition of a ‘Conventional Ship’ is defined by the author as:

A ‘Conventional Ship’ is one that complies with (all) current⁴ regulatory requirements.

The term ‘all’ is bracketed to reflect that flag-states may grant derogations or exemptions from certain statutory provisions. As a result, regulatory interpretations and compliance expectations may vary

⁴ The term ‘Current’ is at the time of writing

across jurisdictions, potentially influencing the type and sufficiency of evidence required for regulatory review. Consequently, the conceptual requirement of ‘Acceptably Safe’, must be validated in accordance with the expectations and frameworks of each regulatory stakeholder.

With the ongoing development of the IMO’s Maritime Autonomous Surface Ships (MASS) Code (see section 2.3.1), the definition of ‘conventional’ is poised to evolve. The MASS Code, once adopted as a mandatory instrument [17], will expand the regulatory framework to explicitly encompass autonomous and remotely operated functions, including requirements for remote operations centres (ROCs), connectivity, and supporting infrastructure. This transition will redefine what constitutes regulatory compliance, extending beyond the vessel itself to include all elements of the Maritime Autonomous Infrastructure (MAI).

As a result, the assurance/safety case for autonomous vessels will need to address not only shipboard systems but also the broader socio-technical context, including land-based operations, cross-jurisdictional legal requirements, and dynamic operational conditions. The concept of “conventional ship” will thus shift from a vessel-centric model to one that integrates autonomy and remote operation as core components of regulatory compliance and safety assurance.

2.3 Current regulatory developments

This section identifies recent research initiatives regarding the Maritime Autonomous Infrastructure (MAI), developments within regulatory authorities and Classification Societies, and assesses how these align with the Lifecycle Process Model (LPM), Safety Process Model (SPM), Design Envelope (MAI-DE), and the Layer of Protection (LoP) framework developed within this thesis.

While remote control of ships is not a novel concept, as evidenced by the conversion of the USS *Iowa*, an 11,410-ton battleship commissioned in 1897 into the U.S. Navy’s first radio-controlled target ship in 1920 [13], the autonomous operation of vessels without crew in international waters introduces a number of unique challenges, including, technical, legal, operational and safety assurance that are not adequately addressed by the existing regulatory frameworks for conventional vessels.

This regulatory gap is not new. A 1964 document published by the Inter-Governmental Maritime Consultative Organization (IMCO – predecessor to the IMO (1982)) document MSC VIII/11 Automation in ships – Note from the Secretariat defined remote control as [14]:

‘Remote control is sometimes used in a partly-automated system. It includes, for example, monitoring of data from machinery operated at a distance from, say, a central control panel or the navigating bridge of a ship, but essentially involves human judgment and operation’.

The statement illustrates the historical presumption that human oversight remained central to vessel operations, even when aided by automation. However, as technological capability progressed, these assumptions began to be challenged.

One of the earliest significant efforts to explore this shift was the MUNIN project (Maritime Unmanned Navigation through Intelligence in Networks), launched in 2012. This was the first European initiative to explore the feasibility of operating crewless and autonomous ships during deep-sea-voyage, but not in congested waters or during approaches [15]. While the limitations of MUNIN included a restricted voyage plan, and that it did not address reasonably foreseeable abnormal or emergency operations, it did include infrastructure elements that extended beyond the vessel, laying the groundwork for the broader concept of the MAI.

Following this Rolls-Royce Commercial Marine announced its vision for maritime vessels operating independent of human control (autonomously) or operating remotely controlled on international voyages with no crew on board [16]. In response, the commercial maritime sector quickly recognised that the existing regulatory framework did not adequately address the introduction of technologies that support such operations.

This led the Maritime Safety Committee (MSC) of the International Maritime Organisation (IMO) to conduct a regulatory scoping exercise (RSE) [17] to examine relevant ship safety treaties on how Maritime Autonomous Surface Ships (MASS) could be regulated in international waters as defined by the United Nations Convention on the Laws Of the Seas (UNCLOS) [18]. The exercise, initiated in 2017 and completed in May 2021, provided the first comprehensive assessment of how existing IMO instruments apply to autonomous and remotely operated vessels, identifying areas where current provisions are adequate, those requiring clarification, and those in need of new or amended

instruments. The findings established the foundation for subsequent IMO work, including the development of the non-mandatory MASS Code marking a formal recognition that autonomy introduces novel operational, and safety assurance challenges not fully addressed by existing conventions.

2.3.1 IMO - Non-Mandatory MASS Code.

Building on the overview provided in Section 2.3.1, this subsection examines the IMO's work on the MASS Code [17], with the intention of establishing a global framework for the safe operation of autonomous ships. The Code is being drafted as a goal-based instrument, meaning it sets high-level safety objectives and functional requirements, rather than prescriptive rules. This approach is intended to accommodate rapid technological innovation and diverse vessel designs, but also introduces complexity in interpretation and implementation. The drafting process involves extensive collaboration among IMO Member States, intergovernmental bodies, and industry stakeholders. The non-mandatory code is seen as an interim step (finalised in 2026), followed by an experience building phase (EBP) and then moving towards a future mandatory instrument (start date of 2028 with adoption in 2030).

While the goal-based approach offers flexibility, it risks ambiguity in enforcement and may lead to diverging interpretations among flag states and or other relevant stakeholders. The absence of detailed prescriptive requirements further complicates verification, particularly for novel technologies and operational models. There is also concern that the Code, in its current form, may not fully address the integration of land-based systems and remote operation centres (ROCs) into the maritime safety regime. Such concerns are grounded in well-established principles of international maritime law, which provide limited mechanisms for regulating the land-based elements that underpin autonomous or remotely controlled operations. Under UNCLOS [23], a flag State's jurisdiction extends to the ship and its activities on the high seas (Articles 92–94), but does not confer authority over land-based infrastructure located in another State's territory. This creates uncertainty where Remote Operation Centres (ROCs) and connectivity services are situated outside the flag State's jurisdiction. Consequently, the IMO, as a regulatory-making body focused on maritime safety, cannot regulate land-based systems directly, and these constraints are recognised in ongoing discussions during the development of the MASS Code.

A critical challenge arises from the IMO's limited jurisdiction over land-based laws and the regulatory frameworks governing communication providers and remote operation centres. If a ROC is located outside the flag state's territory, questions emerge regarding the effective exercise of flag state control, the "genuine link" required by UNCLOS, and the attribution of legal responsibility in case of incidents. Some flag states foresee legal impediments to certifying and overseeing ROCs located abroad, suggesting the need for bilateral agreements or memoranda of understanding to clarify jurisdictional authority.

In conclusion, the development and implementation of autonomy within the maritime sector remains a complex and evolving challenge. While the state-of-the-art frameworks and standards from other domains offer valuable insights, their direct adoption is constrained by the unique regulatory, operational, and jurisdictional complexities of maritime operations. The ongoing work on the IMO MASS Code exemplifies both progress and persistent gaps, particularly in aligning cross-jurisdictional legal requirements and integrating land-based elements into the safety case. Moving beyond the current state of the art will require a fundamental transformation in regulatory assurance processes, one that embraces a holistic, system-of-systems perspective and ensures that the claim of 'Acceptably Safe' is substantiated across all elements of the MAI, not solely the vessel or its ROC.

2.3.2 Demonstrating Feasibility

Concurrently, a number of pilot activities have demonstrated the feasibility of autonomous and/or remotely controlled maritime functionality. Notable examples include the SISU project in Denmark [19], Norway's Yara Birkeland [20] and ASKO vessels [21], as well as the MEGURI 2040 project in Japan [22]. While these initiatives have demonstrated autonomous capabilities, all are currently operating with crew on board to comply with existing regulatory requirements. More advanced implementations include Sea Machines operating around the coast of Denmark [23], and the Reach-Subsea vessel [24], both of which have adopted remote operations from their inception. In 2018, Rolls-Royce and Finferries conducted a high-profile demonstration of the world's first fully autonomous ferry in the archipelago south of the city of Turku, Finland [25], followed by a new research project called SVAN (Safer Vessel with Autonomous Navigation), a continuation of the

Advanced Autonomous Waterborne Applications (AAWA) research project, funded by Business Finland (TEKES)[16].

While these implementations validate the technical viability of remote control and autonomous functionality, the legal operation of such vessels as described in [130], requires structured engagement with Regulatory Authorities, Port and Competent Harbour Authorities, along with legislative measures to address salvage, cargo claims, right of arrest, and product liability. In practice, this has required direct engagement with national maritime regulators to ensure that vessel operations within a flag-state's territorial seas conform to local legislative requirements.

Recognising that the work of the IMO is of pure academic interest for vessels not operating internationally, several national authorities have issued their own requirements for autonomous vessel operations within their jurisdiction. Notable examples include Australia (AMSA) [136], the Norwegian Maritime Authority (NMA) [137], the Danish Maritime Authority (DMA) [138], and the UK Maritime and Coastguard Agency (MCA) [139]. These national frameworks provide pathways to acceptance but, in some cases, diverge significantly from one another.

A consistent requirement across jurisdictions is the use of structured risk assessments; however, the prescribed methodologies, vary:

- NMA: requires a formal Failure Modes and Effects Analysis (FMEA);
- DMA: accepts multiple methods, provided they align with or are mapped to IMO Circular MSC.1/Circ.1455 [26];
- AMSA: lists a range of acceptable techniques, including FMEA, FMECA, FTA, ETA, CRIOP, and O&SHA;
- The European Union guidance: permits any method deemed acceptable by the relevant administration.
- UK-MCA: requires a risk assessment but does not mandate a specific methodology.

Although risk assessments are universally required, there is currently no standardised obligation across these regulatory frameworks to present the outputs of such assessments in a format that is accessible and interpretable by all relevant stakeholders. While methods such as FMEA are intended to capture all failure modes, including those introduced by AI, there is currently limited research in adapting classical safety analysis techniques to address the unique challenges posed by AI driven

functions [27]. This lack of standardisation has been recognised in IMO deliberations. As a partial response, the draft non-mandatory MASS Code includes provisions for the consistent structuring of output data from the IMO MASS experience building phase, including the reporting of trials and safety analysis. However, these provisions operate at the vessel and voyage level and do not extend to the System-of-Systems (SoS) context. As a result, data formats and reporting practices may result in incompatible formats across different subsystems or projects. Such fragmentation hinders effective risk analysis and system integration ultimately impacting the safety assurance of the MAI.

This divergence illustrates the current reliance on negotiated, project-specific acceptance processes, as noted in [8]. In the absence of a unified regulatory methodology, developers and operators of remotely controlled or autonomous systems, are required to negotiate assurance and compliance on a case-by-case basis with national authorities. Without the adoption of a structured process such as the LPM proposed in this thesis, the negotiations risk becoming inconsistent, potentially undermining regulatory confidence, delaying approval, and fragmenting global efforts to introduce autonomy. Such conditions echo historical precedents, where disparate national requirements hindered standardisation, making international trade more difficult. The adoption of a unified, transparent framework is therefore essential to support the safe and efficient integration of autonomous maritime systems.

These pilot projects and regulatory initiatives collectively illustrate the current state of the art in maritime autonomy: technical feasibility has been demonstrated, yet widespread adoption is constrained by fragmented regulatory frameworks, inconsistent risk assessment methodologies, and a lack of harmonised standards for evidence presentation and system integration. The reliance on negotiated, project-specific acceptance processes highlight the absence of a unified regulatory pathway, resulting in uncertainty and inefficiency for developers and operators.

This thesis directly addresses these limitations by proposing a structured, lifecycle-oriented assurance framework, the Lifecycle Process Model (LPM), which integrates vessel, remote operations centre, connectivity, and shore-side services into a coherent system-of-systems approach. By establishing transparent processes for risk identification, evidence generation, and stakeholder engagement, the framework supports the development of defensible assurance/safety cases and facilitates regulatory confidence. In doing so, it advances beyond the current state of the

art, providing a foundation for scalable, internationally harmonised deployment of autonomous maritime systems.

2.4 Current Classification Society developments.

Classification societies play a critical role in shaping safety assurance and system design expectations across the maritime sector. As independent technical organisations, their guidance documents and class notations significantly influence how novel technologies, such as those used for remotely operated and autonomous vessels are developed, assessed and certified. However, despite their shared membership in the International Association of Classification Societies (IACS) [28], their approach to autonomy varies considerably. This divergence has created uncertainty regarding the nature and sufficiency of evidence required to achieve classification acceptance, particularly in the context of the MAI, and further exacerbates the risk of a fragmented assessment and regulatory landscape.

Note that IACS explicitly state that class certificates do not guarantee safety, fitness for purpose, or seaworthiness, and that they have no control over how a vessel is operated and maintained between surveys [131]. For crewless operations, this disclaimer becomes even more consequential.

The removal of Standards of Training, Certification and Watchkeeping (STCW)-trained personnel as an on-board Layer of Protection shifts the assurance burden from continuous human oversight to design-time and shore-side controls. These include inherently safe design, Remote Operations Centre (ROC) procedures, connectivity performance, remote diagnostics, and where required automated recovery. As a result, reliance on class certification alone is insufficient to demonstrate that a MAI is ‘Acceptably Safe’ for a given voyage. From a state-of-the-art perspective, this creates:

- (i) An evidence sufficiency gap between design/class compliance and the operational evidence required to justify that the MAI remains ‘Acceptably Safe’ to operate within a defined context of use.
- (ii) A responsibility allocation gap across the vessel, ROC, connectivity providers, and maintainers within a system of systems context, and
- (iii) A temporal gap between periodic surveys and continuously evolving operational conditions.

Notably, several IACS members have issued guidance documents and class notations for remote and autonomous systems, reflecting different assumptions, evidence requirements, and assurance expectations. This variation highlights the absence of a harmonised framework and the need for greater alignment among classification societies to support consistent outcomes for remote and autonomous operations. Together, these interrelated gaps reflect the need for ongoing validation of safety claims as system configurations evolve. They also highlight the limitations of existing vessel-centric assurance frameworks and establish the rationale for the development of the LPM.

The following examples illustrate the diversity of current Classification Society approaches include:

Lloyd's Register (LR)

- **2016 – ShipRight Procedure: Autonomous Ships [29]**
 - Defined seven levels of autonomy.
 - Required a risk-based approach, recommending FMEA or equivalent methods aligned with national or international standards.
 - Addressed Human Centred Design (HCD), data assurance, and system security.
 - Cited relevant international standards. [30][31][32].
- **2019 – Digital Descriptive Notes [33]**
 - Revised procedure based on six Accessibility Levels (AL) for assigning digital descriptive notes for autonomous or remotely accessed ships.

China Classification Society (CCS)

- **2018 – Guidelines for Autonomous Cargo Ships,– Rules for Intelligent Ships [34].**
 - Defines **three autonomy levels**, all requiring remote control and monitoring capability.
 - Includes provision for **emergency anchoring**, mandating remotely operated chain release mechanisms.
 - However, **no guidance on** emergency anchoring to explain what happens if there is a loss of connectivity, preventing the remote operation of the chain release device.

American Bureau of Shipping (ABS)

- **2024 – Autonomous and Remote-Control Functions** [35]
 - A **goal-based framework** defining three levels: *Smart*, *Semi-Autonomous*, and *Autonomous*.
 - Explicitly states that autonomy **does not imply an unmanned vessel**.
 - Risk classification is based on **operational supervision levels** and **consequence categories**.
 - Risk assessment techniques must be **appropriate for the intended function**.
 - Requires the possibility of a human retaking control.

Det Norske Veritas (DNV)

- **2024 – Autonomous and Remotely Controlled Vessels** and related class notations [36]
 - Requires a **risk assessment** but **does not prescribe a specific methodology**.
 - Class notations are based on four modes of operation and three locations of control.
 - References several international standards, including [30][31][32][37]

Bureau Veritas (BV)

- **2017 – Guidance for Autonomous Ships** [38]
 - Requires a **qualitative risk assessment** to be carried out.
 - ALARP principle defined in the document, risk mitigation founded in prescriptive requirements.
 - Demonstration of equivalence to existing systems
 - Defines **five autonomy levels**.
 - Cited relevant international standards. [30][31][39].

Despite all societies requiring some form of risk assessment and referencing overlapping international standards, there remains no unified approach to methodology, autonomy level definitions, or expectations for safety evidence. For example, only some explicitly address human-centred design or fallback strategies in the event of a loss or degradation of control, and none prescribe how assurance arguments should be structured to ensure transparency or cross-stakeholder interpretability.

This fragmentation poses a significant challenge for developers of the MAI, as the sufficiency and format of evidence becomes dependent on the specific classification society engaged. Without harmonisation or mutual recognition of assurance frameworks, each project is forced to navigate a bespoke path towards acceptance, resulting in inconsistent requirements, varying interpretations of safety, and elevated uncertainty. Notably, Classification engagement is not mandatory for all vessels, particularly those operating exclusively within national waters.

As a result, most Classification Societies have opted to publish guidance documents and not enforceable rules. While this provides flexibility, it also introduces variability in how such guidance is applied, often depending on the assessor's individual expertise in complex SoS, assurance/safety case and MAI environment. This variability can result in uncertainty in the claim of 'Acceptable Safe' for the MAI, which this thesis aims to address.

This thesis addresses these risks through a goal-based and argument-led assurance/safety case approach, supported by the LPM. It incorporates explicit layers of protection (LoP) that do not assume or rely on immediate human intervention, per-voyage validation of fallback states, and Design Envelope (MAI-DE) constraints that must be satisfied before and during operations. Together these elements bridge the identified assurance gaps and support a robust foundation for the 'Acceptably Safe' deployment of autonomous maritime systems, aligning with emerging best practice and anticipated regulatory developments such as the IMO MASS Code.

2.5 Autonomy in other transportation domains.

This section examines the state-of-the-art in autonomy across rail, aviation, and the automotive sector. It distinguishes established technological advances and unresolved challenges in these domains that are analogous to those faced in the maritime sector. By drawing these comparisons, the section identifies potential solutions and lessons that could inform the development of maritime autonomy.

Rail transport has seen the most success in introducing automation, with a fully automated mail railway system installed in London in 1927. In passenger transport, notable examples include London's Docklands Light Railway (DLR) designed for automation from the outset (operational in 1987) and Paris's Line 1 which was an upgrade of an existing railway (operational in 2011) [40][41]. Today, many metro systems, particularly in Asia operate at Grades of Automation (GoA) 3 OR 4 [42]. These systems operate in highly constrained environments with the benefit of signalling systems to control movement. There are also support staff, e.g. dispatchers for the DLR to check that the situation on the platform is safe for the train to start to move (a function normally carried out by drivers). There has been work on automation of urban and inter-urban rail, but to the authors knowledge there are no operational rail systems that meet the definition of autonomy, in the sense of operating independently across unconstrained networks without continuous human oversight.

In aviation, there is a growing introduction of 'drones', small, uncrewed aerial vehicles that can carry small payloads, e.g. for delivering supplies or for reconnaissance. The military also operate unmanned aerial vehicles for reconnaissance and for offensive roles. In many cases, these systems are remotely piloted, not autonomous, and there have been many instances of losses, for example, the UK's Watchkeeper surveillance drone operated by the Army has experienced multiple accidents some due to mis-operation, showing the difficulty of managing remote operations [43]. Attention is being given to automation for passenger-carrying air vehicles, for example electrical vertical take-off and landing (eVTOL) air taxis. Perhaps the most advanced is Eve Air Mobility who have produced a flyable full-scale prototype [44], even this, however, is intended to be piloted before approval can be gained for autonomous flight, and no timelines for that are quoted publicly. Full autonomy in passenger aviation remains a future goal, with current deployments focussed on cargo, surveillance, and limited urban mobility.

The automotive sector has served as the principal test bed for highly automated operations, with Waymo leading the way, providing driverless taxi services in several US cities, e.g. San Francisco. Whilst what Waymo has achieved is remarkable, the vehicles are operated within tightly defined operational design domains (ODDs). These services do however illustrate technical feasibility where systems are engineered for bounded environments and are initially deployed in relatively benign environments, e.g. Arizona, before being progressively updated to deal with the fog and rain in San Francisco [45].

Despite these advances, many companies have sought to produce similar capabilities, e.g. Cruise, a subsidiary of General Motors focussed on urban robotaxi deployment but faced significant safety and regulatory setbacks, culminating in a nationwide operational suspension and eventual withdrawal from autonomous taxi development [46]. The sector continues to illustrate the commercial difficulties of achieving sustainable success, and many start-ups have either failed or been bought by other players. Several of the major OEMs have started their own activities only to shut them down, writing-off substantial investments [47].

These developments highlight a broader risk when introducing emerging maritime autonomous capabilities. Firstly, there is a lifecycle mismatch, the automotive sectors commercial and technological turnover can occur within just a few years, whereas ships typically have a lifespan of 30 years. For the MAI this disparity creates a significant assurance challenge as the through life assurance/safety case-must therefore explicitly consider obsolescence across all elements of the MAI.

There are notable commonalities across transportation domains, in the classification of autonomy, typically through formal levels or grades. In rail, the Grades of Automation (GoA) framework is widely adopted, while the automotive sector relies on SAEJ0316 [132] standard to define levels of driving automation (usually just referred to as levels). Currently, most automotive activities operate at level 2 – partial driving automation – where the vehicle can steer, accelerate and decelerate, but the driver remains responsible for overall control. The landscape is further complicated by manufacturers claiming their systems are level 2+, or level 2++, which blur the boundaries between established definitions. In contrast, the UK's Autonomous Vehicles (AV) Act eschews levels, and classifies vehicles as self-driving or not, with the operator or manufacturer responsible for safe driving in the former

case [48]. Similar classification challenges are seen in rail, where alternative classification schemes for automation have been proposed, such as those in China, which is at the forefront of introducing autonomy on its metros.[49]

Despite these frameworks, the focus remains predominantly on the development of the vehicle itself – indeed the term ‘ego vehicle’ is widely used in road transport where the intent is that each vehicle can operate by itself, rather than being part of a wider ecosystem. In practical terms, these developers see remote assistance as a transitional phase to full autonomy, however, none of them extend to a comprehensive infrastructure perspective analogous to the maritime autonomy infrastructure (MAI). Consequently, this research adopts a unique perspective, emphasising the necessity of a SoS Assurance approach and highlights the limited opportunity to draw directly on successes in other domains.

There are other important differences between the maritime sector and the other transportation domains, particularly in terms of environmental and operational constraints. Unlike road transport, where the infrastructure remains fixed and predictable, the maritime environment is inherently unstructured and dynamic. For example, image analysis for object detection and avoidance for cars does not have to deal with the effect of waves masking other vessels or objects, coating lenses with salt, thus degrading optical clarity, or lens obstruction caused by ice or spray. Similarly, while the aviation sector encounters communication challenges over long distances [50], emerging autonomous system such as eVTOL aircraft, are intended for urban operations where connectivity is relatively stable and controllable [51]. In practical terms this means that advanced technologies, e.g. for image analysis in cars, cannot simply be migrated across into the maritime domain, although some of the principles, e.g. for avoiding single points of failure in aircraft, can be brought across.

Further, the maritime domain presents unique operational challenges that are not directly comparable to those encountered in other transport sectors, particularly in relation to maintenance and fault management during a voyage. In the automotive domain, vehicles experiencing faults can typically come to a stop in a safe location and await assistance. In aviation, commercial aircraft are designed with a level of fault-tolerance to enable them to complete safe flight and landing, followed by maintenance action on the ground. Similarly, rail systems incorporate both fault-tolerance and regular preventative maintenance activities (as do aircraft) [52]

In contrast, maritime operations, especially those involving crewless autonomous or remotely operated vessel functions, must account for the possibility of extended durations at sea, far from human intervention or infrastructure support. This creates a distinct requirement to design systems that can manage degraded modes, conduct autonomous diagnostics, and ensure continued safe operation without immediate human intervention. There is no direct analogue in the other transportation domains for this requirement. Thus, the need to consider autonomy in regards of management of systems, and system level resilience in the design and assurance of the MAI has no real counterpart in other domains, and this further underscores the novelty of the work presented in this thesis.

The report on the closure of Heathrow Airport [53] on the 21 March 2025, stated that *“employees believed”* the electrical power system was a resilient system, due to it having three separate intakes from the national grid. However, the report also identified interdependencies between assets, such as *“overheating in the server room which resulted in lost access to the capability to remotely connect to certain systems”*. This example illustrates the critical need to move beyond perceived resilience and instead adopt an explicit, evidence-based definition that is tailored to the unique characteristics of the MAI.

Within the context of the MAI, resilience must be explicitly defined, agreed upon at the project inception, and supported by demonstrable evidence. The early identification of critical interdependencies, whether technical, organisational, or procedural, must be embedded into early-stage planning, design, and assurance activities to control system complexity, mitigate emergent risks and ensure coherent safety assurance across a distributed and interdependent system-of-systems (SoS).

The LPM proposed in this thesis provides a structured methodology that facilitates the systematic identification and analysis of interdependencies throughout the MAI’s lifecycle, enabling stakeholders to transition from subjective beliefs to demonstrable, maintainable resilience and risk control.

In summary, while significant progress has been made in the automation and remote operation of rail, aviation, and automotive systems, these advances remain bounded by domain-specific constraints and do not fully address the unique challenges faced by the maritime sector. The maritime

environment's inherent unpredictability, the extended operational lifecycles of vessels, and the imperative to consider the entire supporting infrastructure, not just the vessel itself, place the Maritime Autonomous Infrastructure (MAI) beyond the current state of the art in other domains.

While certain principles can be drawn from other domains, such as sensor fusion, remote supervision and over the air updates, to inform maritime autonomy, the MAI requires a goal based, life-cycle assurance approach that accepts technological developments, maintains independence of layers of protection, and sustains a defensible claim of 'Acceptably Safe' across evolving operational and regulatory conditions. Where, relevant, this thesis identifies and adapts emerging technology-level standards, such as ISO PAS 8800 on safety and AI for road vehicles [54], as well as established practices like inherently safe design, to support the development of robust assurance frameworks for maritime autonomy. In doing so, this work moves decisively beyond the boundaries of existing industrial practice and advances the field by proposing a structured, lifecycle-oriented assurance framework tailored to the distinctive requirements of maritime autonomy.

2.6 Academic state of the art research

Building on the historical, regulatory, technical, and industrial perspectives outlined in the preceding sections of this chapter, this section provides a critical analysis of the academic literature on maritime autonomy. While earlier sections have mapped the evolution of industry practices and regulatory frameworks, this section evaluates the current state of scholarly research, highlighting both the progress made and the persistent limitations of vessel-centric approaches. By identifying key gaps, particularly the absence of integrated, infrastructure-level assurance frameworks, this review establishes a clear rationale for the novel system-of-systems perspective and methodologies advanced in this thesis. In doing so, it ensures that the literature survey not only documents the development of the field but also directly informs and justifies the research direction and original contributions that follow, specifically addressing the broader MAI.

At the outset of this research, very few publications addressed the broader assurance/safety challenges associated with operating crewless or remotely controlled vessels within a regulated maritime environment, and none considered these at the MAI level. Furthermore, to the best of the authors knowledge, the existing literature has not considered the dynamic and evolving safety assurance process, changing regulatory requirements, jurisdictional differences and the complexities

of transitioning between voyage or operational conditions, issues that are explicitly addressed within this thesis.

Early academic contributions to maritime autonomy were limited in scope and largely focused on the technical feasibility studies of remote or autonomous navigation, often addressing isolated system elements such as collision avoidance [55] [56] [57] [58]. Projects such as MUNIN [15] and AAWA [16] laid the foundation for conceptualising autonomous ships as integrated control platforms. However, these initiatives did not consider the wider socio-technical considerations of the MAI, nor did they consider the dynamic regulatory requirements, changing stakeholder community or assurance/safety requirements when operational conditions change.

At the boundaries of current literature, several studies have begun to consider the Remote Operations Centre (ROC) and connectivity as elements within the broader context of the MAI, including the work presented in [59] [60] [61]. However, these contributions do not sufficiently address the risks associated with the operation of the MAI under Reasonably Foreseeable Abnormal Event (RFAE) and emergency conditions.

Two notable contributions to the academic research on maritime autonomy include the work in [59] which conducted a comprehensive bibliometric review encompassing 417 publications issued between 2011 and 2022. Their analysis identified three predominant research themes within the field:

- Safety engineering and risk assessment to support decision-making,
- Navigation safety and collision avoidance, and
- Cybersecurity risk analysis.

The review also highlights the need for further research in areas such as unmanned machinery operations, online risk tools, the application of system-theoretic safety methodologies, human factors integration, and the development of suitable risk acceptance criteria tailored to the safety assessment of autonomous vessels.

The second paper [60], categorises the safety challenges for Maritime Autonomous Surface Ships (MASS) into three main groups:

- Technological Challenges: Issues related to hardware and software reliability.
- Human Factors: Challenges arising from human-machine interaction, including situational awareness and decision-making.
- Procedural Challenges: Difficulties in integrating MASS into existing maritime procedures and regulations.

The authors emphasise the qualitative nature of collision regulations (COLREGs) and the need for further research to ensure autonomous ships comply with legal requirements that are open to interpretation, such as COLREG Rule 6 and the requirement to ‘proceed at a safe speed’, without quantifying what is meant by ‘safe speed’.

While both papers provide valuable insights into the safety, reliability, and risk assessment challenges, the prevailing literature remains primarily vessel-centric. These studies focus on shipboard systems, collision avoidance, human-machine interaction at the vessel level, and procedural compliance within existing maritime conventions. However, they do not extend their analysis to encompass the broader socio-technical environment in which these vessels operate. Notably absent is any structured treatment of the supporting infrastructure, such as remote operations centres (ROCs), communications networks, digital support services, or the institutional and regulatory frameworks that enable autonomous vessel operations.

A further systematic review carried out in 2025 confirmed there were sporadic papers between 2016-2018 using COLREGS to guide the technical developments of autonomous functionality and derive test scenarios for evaluating their systems [62].

In contrast, to advance the state-of-the-art, this thesis introduces the concept of the MAI as a distributed, socio-technical system of systems. It defines a LPM that explicitly accounts for the dynamic interaction between technical subsystems, human actors, legal requirements and evolving operational contexts. This approach enables a more comprehensive safety analysis, extending beyond the vessel to include fallback strategies, control transitions, stakeholder roles, and regulatory alignment over the full system lifecycle.

By addressing the critical gaps in the existing literature particularly the lack of integrated, infrastructure-level assurance frameworks, this research offers a novel and structured methodology for understanding and assuring safety across the entirety of the MAI, rather than limiting analysis to the autonomous ship in isolation. In doing so, it advances the academic state of the art and provides a foundation for future regulatory harmonisation, industry best practice, and the scalable deployment of maritime autonomy.

2.6.1 Applicability of cross-sector assurance frameworks.

Recent academic research has developed processes that can support the creation of the compelling body of evidence that is required to be submitted to the regulatory bodies for regulatory review. Cross-sector frameworks such as the Guidance for the Safety Assurance of Autonomous Systems in Complex Environments (SACE) [63] and Assurance of Machine Learning in Autonomous Systems (AMLAS) [64] can be applied within the MAI process, however, SACE assumes that:

“a systems safety process is already in place”,

and AMLAS requires that:

“system-level safety requirements, including acceptable risk targets, are a fundamental input to the AMLAS process. These requirements are expected to be generated by domain experts or derived from the relevant regulatory requirements.”

Both requirements will be challenging, as system safety processes within the maritime sector are either fragmented or do not exist. Additionally, the maritime sector faces difficulties in deriving system level safety requirements at a SoS level, particularly when applied to the MAI.

In summary, while cross-sector assurance frameworks provide valuable methodological insights, their practical implementation in the maritime domain is constrained by the absence of unified LPM and SPM at a SoS level. The existing academic research remains predominantly vessel-centric, with only limited consideration of broader issues such as human-centred design, cybersecurity, remote operations centres (ROCs), connectivity, and shore-side services. Addressing these gaps is central

within this thesis developing a comprehensive assurance approach for the MAI and supporting the claim of ‘Acceptably Safe’.

2.6.2 Future Academic Research Directions and Responsibility Gap

While this thesis advances the state of the art by introducing a system-of-systems perspective and a structured assurance methodology for the MAI, future academic research in maritime autonomy must grapple with the profound influence of historical practices and entrenched jurisdictional barriers. The legacy of vessel-centric regulation and assurance frameworks presents both a challenge and an opportunity: new methodologies must be compatible with established conventions while enabling a transition to more adaptive, infrastructure-level approaches. Jurisdictional fragmentation where authority is divided among flag states, port states, and international bodies, demands the development of assurance processes that are portable, mutually recognised, and capable of resolving regulatory conflicts. Equally, the complexity of stakeholder relationships and shifting power dynamics in the MAI SoS require transparent allocation of responsibility and liability, as well as inclusive engagement strategies that reflect the interests of all affected parties.

Recent literature has highlighted the growing complexity of assigning responsibility in the development, deployment, and assurance of autonomous systems [65][66]. Three systemic gaps were identified that pose challenges to the safe deployment of autonomous systems: these were identified as the ‘*semantic gap*’, the ‘*responsibility gap*’, and the ‘*liability gap*’. These gaps reflect the misalignment between system intent and actual behaviour, the ambiguity in assigning moral responsibility, and the uncertainty in establishing legal liability. While their framework is not specific to maritime systems, its implications for the MAI are substantial.

The LPM developed in this thesis addresses the ‘gaps’ by embedding iterative validation strategies, allocating stakeholder responsibilities across system boundaries, and integrating compliance mechanisms to support legal and moral accountability. These measures collectively enable the development of defensible assurance/safety cases. Together, the LPM, SPM, MAI-DE and LoP frameworks form the foundation of a structured and holistic approach to managing the assurance obligations of the MAI throughout its operational lifecycle.

Overcoming cultural and institutional inertia will be essential, necessitating demonstration projects and regulatory sandboxes such as the North Sea MoU established in 2025 to build trust and facilitate change [133]. As the MAI evolves dynamically across operational contexts and legal boundaries, assurance cases must become living documents, supported by digital tools and AI-driven systems that enable real-time updating and validation.

Finally, future research must address the ethical, social, and environmental dimensions of maritime autonomy, ensuring that assurance frameworks reflect societal values, define acceptable risk in novel contexts, and uphold the sector's longstanding commitment to safety and environmental stewardship. By integrating these considerations, the next generation of academic inquiry can support the safe, scalable, and socially responsible deployment of autonomous maritime infrastructure.

Several important avenues remain for academic exploration beyond the current state-of-the-art, including:

- a. **Consistency and Standardisation of Assurance Outputs:** There is a need to expand upon this research to develop processes that consistently produce assurance cases and safety evidence in formats recognised and understood by regulators across jurisdictions. Future work should focus on harmonising outputs and developing digital platforms that facilitate transparent, auditable, and updatable assurance documentation.
- b. **System-of-Systems Analysis Across Technical, Jurisdictional, and Operational Boundaries:** Further research should deepen the system-of-systems approach, explicitly modelling and analysing interactions between vessels, remote operations centres, connectivity providers, and shore-side services. This includes understanding how technical changes, regulatory requirements, and operational transitions (such as port entry or emergency handover) impact overall safety and assurance.
- c. **Artificial Intelligence for Assurance Case Generation and Evaluation:** Research should investigate how AI can integrate, analyse and synthesise conclusions from operational data, regulatory requirements, and incident histories to automate the generation of assurance/safety cases. Additionally, AI could be leveraged to continuously evaluate and adapt assurance/safety cases in response to changes during a single voyage, supporting real-time risk management and decision-making.

- d. **Defining “What Good Looks Like” for Regulatory Confidence:** Academic research should engage with regulators, industry, legal, insurers, operators, designers and other stakeholders to define acceptable risk levels, transparency requirements, and auditability requirements that provide sufficient confidence for certification and operational approval.
- e. **Simulation-Based Approaches:** Advancing the use of simulation for testing, validating, and certifying autonomous systems under diverse scenarios will be essential for scalable and adaptive assurance.

By integrating these considerations, the next generation of academic inquiry can further support the safe, scalable, and socially responsible deployment of autonomous maritime infrastructure.

2.7 Literature Survey Conclusion

The review of historical, regulatory, and classification society developments reveals a maritime sector deeply rooted in legal traditions and risk mitigation practices that assume the continuous presence of onboard personnel. However, these foundational assumptions are increasingly challenged by the emergence of crewless and remotely operated functions. Despite recent efforts by the IMO, national authorities, and classification societies to respond to these developments, the absence of harmonised definitions, safety criteria, and structured assurance methodologies has resulted in fragmented and inconsistent approaches to risk evaluation and regulatory acceptance.

While many classification societies have issued guidance, these documents often lack enforceability and standardised output expectations, leaving interpretation and judgement to individual assessors. Critically, none of the reviewed frameworks sufficiently addresses the integrated and evolving nature of the MAI, especially under changing voyage or operational conditions.

In addition, comparative analysis across transportation domains highlights the unique operational, environmental, and assurance challenges faced by the maritime sector, particularly the need for analysis of infrastructure dependencies, none of which are comprehensively addressed in other sectors. Recent events such as those at Heathrow, highlighted the need to correctly identify the relevant stakeholders, understand the interdependencies between the various sub-systems, and

ensure the approach to resilience is clearly defined and agreed upon by all relevant stakeholders, which is critical for demonstrating how the claim of ‘Acceptably Safe’ can be met.

Academic contributions have focussed on vessel level automation and technical feasibility, with limited attention given to the broader socio-technical system that characterises the MAI. Theoretical frameworks addressing responsibility, liability, and semantic gaps in autonomy have emerged, but these are not yet integrated with maritime specific assurance/safety obligations. Furthermore, while recent work has begun exploring assurance methodologies for AI, there remains a lack of adaptation to maritime specific hazards.

The existing literature on maritime autonomy has made important contributions in areas such as vessel design, sensor integration, and regulatory scoping. However, a critical gap remains in addressing the safety assurance of the MAI as a holistic system-of-systems. Much of the current research focuses narrowly on the vessel, often in isolation from its supporting infrastructure, and tends to overlook the complex interdependencies and accountability structures spanning organisational, technical, and jurisdictional domains. This thesis responds to that gap by defining the MAI as a system-of-systems and developing an integrated, structured framework for its safety assurance across the full operational lifecycle. Through the development of the LPM, supported by the SPM, the MAI-DE, and the LoP model, this research enables the systematic identification of interdependencies, allocation of stakeholder responsibilities, and iterative validation of assurance activities.

These contributions collectively support the development of defensible and maintainable safety assurance cases that extend beyond the autonomous or remotely controlled functions of the vessel to encompass the wider socio-technical infrastructure. While the framework provides a rigorous foundation for managing the safety and accountability obligations of the MAI, it also acknowledges ongoing uncertainties surrounding regulatory alignment and stakeholder acceptance, highlighting areas for future research and development.

2.7.1 Beyond the State of the Art and Identified Gaps

Critically, there is a lack of research addressing the MAI as a holistic, dynamic system-of-systems. Existing frameworks do not sufficiently account for the evolving nature of operational contexts, the need for continuous assurance across the asset lifecycle, or the complex interdependencies between technical, organisational, and regulatory domains.

There has been some academic work on adapting classical hazard and safety analysis methods for AI and autonomy [27], which would be required to generate the body of evidence necessary to support the claim of ‘acceptably safe’. To the authors knowledge, none of this work has addressed the specific of the maritime environment, e.g. how waves and sea spray may affect AI based image analysis and classification. Whilst an important area, such detailed analysis lies outside the scope of this thesis.

Furthermore, current approaches rarely integrate stakeholder-derived criteria for safety, nor do they provide mechanisms for managing assurance evidence as the MAI configuration changes over time and across jurisdictions. The literature also falls short in adapting assurance methodologies for emerging technologies such as AI, particularly in the context of maritime-specific hazards and resilience requirements.

This thesis explicitly addresses these gaps. It proposes a structured, lifecycle-oriented assurance framework that:

- Treats the MAI as a distributed, socio-technical system-of-systems.
- Embeds stakeholder engagement and responsibility allocation throughout the lifecycle.
- Provides mechanisms for dynamic, per-voyage assurance and evidence management.
- Integrates layers of protection and fallback strategies that do not rely on immediate human intervention.
- Adapts and extends assurance methodologies to address the unique challenges of autonomy, AI, and resilience in the maritime domain.

By doing so, this research not only responds to the limitations identified in the literature but also establishes a foundation for future regulatory harmonisation, industry best practice, and the safe, scalable deployment of maritime autonomy.

To advance this contribution, the next chapter examines the evolving safety paradigms that inform the shift from conventional crewed shipping to the MAI. It evaluates the fundamental differences in operational context, risk ownership, system boundaries, and assurance requirements between traditional vessels and the MAI. This comparative analysis provides the conceptual foundation for understanding why established safety approaches may be insufficient or inapplicable, thereby justifying the need for the new frameworks proposed in this thesis.

Chapter 3 : Evolving Safety Paradigms

This chapter undertakes a comparative analysis of the challenges associated with achieving acceptance for conventional ships and the Maritime Autonomous Infrastructure (MAI). Particular attention is given to the differing approaches to safety assurance, regulatory compliance, and stakeholder engagement. The aim is to explore how current practices may need to evolve to accommodate unique challenges and risks introduced by autonomous and remotely operated functions.

While conventional ships benefit from a long-established framework of prescriptive regulations, classification rules, and national legislation that supports consistent evaluation and certification of design, construction, and operation, the MAI introduces fundamentally different challenges. In contrast, the MAI presents a complex socio-technical system with unprecedented regulatory and operational challenges due to its distributed, cross- jurisdictional nature and reliance on emerging technologies. Addressing these challenges requires a shift from rule-based compliance to an assurance/safety case approach that considered all elements of the MAI, the entire lifecycle, and operational context.

3.1 What is a Maritime Autonomous Infrastructure (MAI).

This section builds upon and amplifies the concept of the Maritime Autonomous Infrastructure (MAI) introduced in Section 1.1, and further elaborates on its constituent elements, which include, but are not limited to:

- The vessel/ship
- Vessel/ship systems, including essential and non-essential services.
- Land-based remote operations centre (ROC).⁵
- Connectivity solutions (e.g. satellite and terrestrial communications infrastructure)
- Human – includes all relevant stakeholders.
- Port and harbour services, including Pilotage and Vessel Traffic Services (VTS).

⁵ ROC – Facility used to support remote control functions. Derived from ISO/TS 23860- 2020

- Emergency response services
- Supporting land-based infrastructure and services.

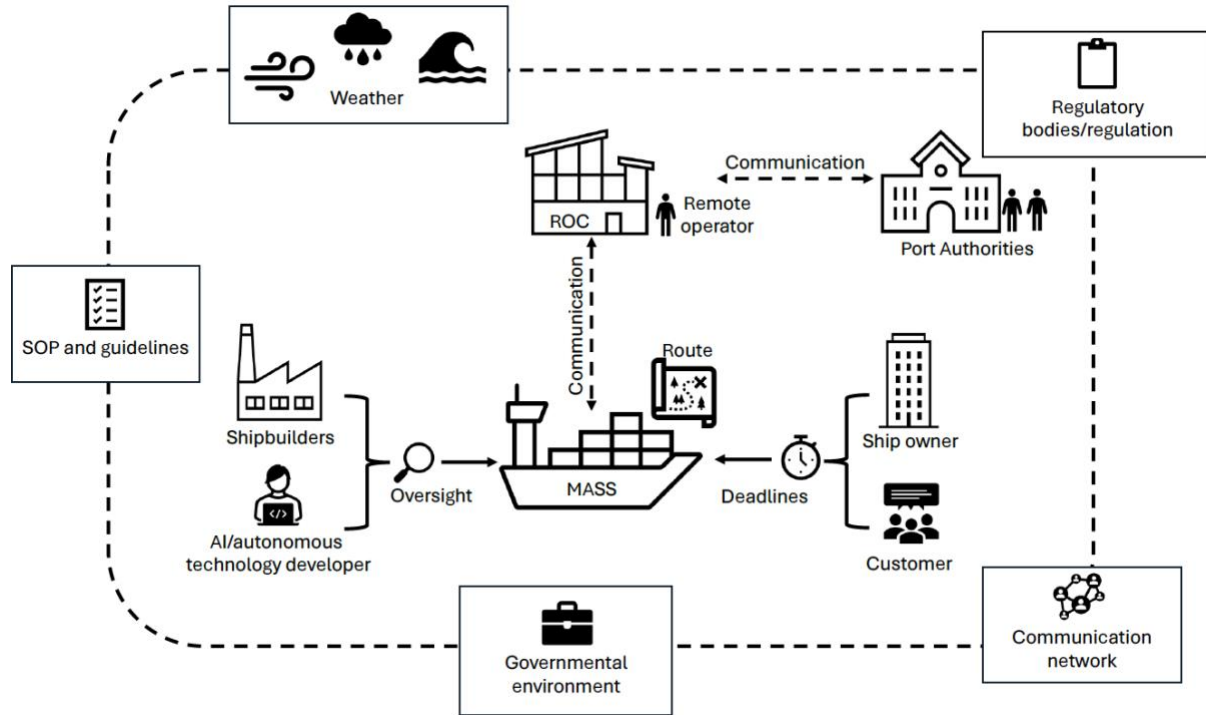


Figure 3-1 Conceptual elements of the Maritime Autonomous Infrastructure:

Courtesy of Dr Kate Preston

It is important to note that the MAI necessarily extends beyond the vessel itself to constitute a broader socio-technical system as shown in Figure 3-1. The exact configuration and identification of its elements must be determined through systematic engagement with relevant stakeholders, recognising that the MAI's composition may evolve during a single voyage in response to technical, operational, or regulatory requirements.

3.1.1 MAI Unique Risks.

This research identified a range of unique risks associated with the MAI by conducting a detailed analysis of individual elements and their potential impact on safety and environmental outcomes in the event of system failure or degradation of the function. For example:

- **The loss of situational awareness:** This could present a potential risk if the system cannot perceive or interpret its environment which could result in collision or grounding.

- **The loss of connectivity:** This risk should be analysed with respect to the context of use.
- **Inability to regain control:** This is use-case dependent and could result in an intolerable risk where remote control of the function is required to ensure safety.
- **Inability to isolate autonomy:** This may lead to significant safety implications when humans are interacting with the technologies on board the vessel.
- **Inability to verify autonomy isolation:** This is a potential risk during maintenance operations or attempting rescue/recovery of a vessel
- **Inability to safely reinstate autonomy:** this may put undue pressure on remote operators and complicate risk mitigations during fallback operations.
- **Inability to identify a decrease in medical fitness of a remote operator:** Unlike a conventional ship, where a decrease in medical fitness and the ability of the individual to discharge the responsibility of their position is normally assessed by the colleagues on board. We can reasonably expect remote operators to leave the ROC at the end of their shift. This may or may not make it more difficult to detect fitness impairment that could potentially lead to an intolerable risk. It should; be noted that the European Aviation Safety Agency (EASA) has addressed this risk and provides guidance to air traffic controllers in deciding whether expert aero-medical advice is needed [68].
- **Not taking a SoS perspective on the three primary elements:** A failure to consider the three primary elements of the MAI which includes the vessel, ROC and connectivity solutions as a SoS could make the claim of 'Acceptably Safe to operate in a defined context of use' difficult to achieve.
- **Failure to detect degradation of the MAI functions** – Detecting functional degradation within the MAI may necessitate the correlation of data across multiple elements of the MAI. If such data correlation is not adequately addressed within the LPM, the claim of 'Acceptably Safe' may not be justifiable.
- **Cyber security:** A malicious cyber-attack may have an impact on safety. Although this is not a unique risk for the MAI, the attack surfaces can increase when operating a vessel remotely from a ROC.

Given that the list of unique risks associated with the MAI is not exhaustive, the process of hazard identification under normal, reasonably foreseeable abnormal and emergency conditions, must remain a continuous and iterative activity throughout the entire lifecycle process. This ensures that

emerging risks are promptly identified, assessed and managed as the operational context evolves see Figure 5- Safety Process Model (SPM) for the MAI.

As stated in Chapter 5, this research provides a framework that supports the development of a compelling body of evidence for regulatory acceptance. As illustrated in Figure 3-2 below, the overarching safety objective Goal (G0) asserts that:

(X) is 'Acceptably Safe' to operate within a defined use case in a given environment,

where (X) is the MAI or a conventional ship. While this goal applies to both, the challenge lies in how this claim is demonstrated through appropriate evidence and assurance processes

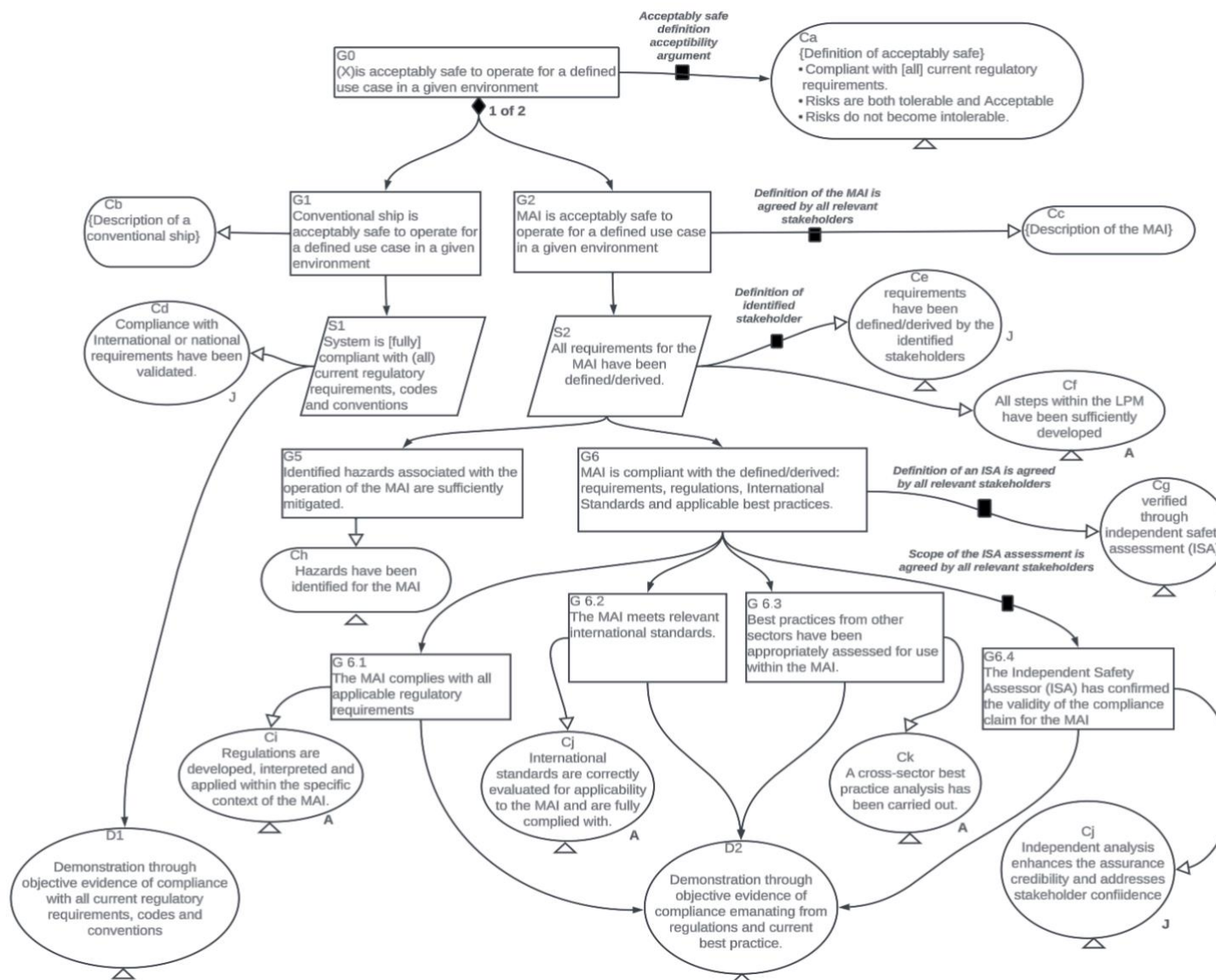


Figure 3-2 Conceptual framework for defining 'Acceptably Safe' in the context of a conventional ship (G1) and the MAI (G2)

For **conventional vessels**, the assurance process is achieved through the following:

G1– Conventional ship is acceptably safe to operate for a defined use case in a given environment.

S1 - System is fully compliant with (all) current regulatory requirements, codes, and conventions, such as those defined in SOLAS.

D1 – Demonstration through objective evidence of compliance with (all) current regulatory requirements, codes and conventions. As the current requirements are prescriptive, verification of compliance is relatively straightforward. The objective evidence of D1 allows the regulatory authorities to issue the necessary certificates for operation of the vessel.

For the **MAI**, the assurance process requires compliance with the following process:

G2 – MAI is acceptably safe to operate for a defined use case in a given environment.

S1 - All requirements for the MAI have been appropriately defined or derived.

Given the absence of comprehensive prescriptive requirements for remotely controlled or autonomous operation of maritime systems, this necessitates a systematic process that ensures all relevant stakeholders are accurately identified and actively engaged in the requirements elucidation process.

D2 – Demonstration through objective evidence of compliance emanating from regulations and current best practice.

Goal G5 – Identified hazards associated with the operation of the MAI are sufficiently mitigated. The principle of '*sufficiently mitigated*' is linked to the tolerability of risk defined by the relevant stakeholders (see Section 5.2.2).

Goal G6 – The MAI is compliant with the defined/derived requirements, regulations, International Standards and applicable best practices, which are broken down into the following Sub Goals:

Sub Goal G 6.1:

Claim: The MAI complies with all applicable regulatory requirements:

Assumption: Regulations are developed, interpreted, and applied within the specific context of the MAI.

Evidence: Mapping the MAI to the applicable regulations.

Sub Goal G 6.2:

Claim: The MAI meets relevant international standards.

Assumption: International standards are correctly evaluated for applicability to the MAI and are fully complied with.

Evidence: The MAI satisfies the relevant international standards such as IEC and ISO.

Sub Goal G 6.3:

Claim: Best practices from other sectors have been appropriately assessed for use within the MAI.

Assumption: A cross-sector best practice analysis has been carried out.

Evidence: An assessment is carried out by an expert review panel confirming relevance and appropriateness of selected best practices.

Sub Goal G 6.4:

Claim: An independent safety assessment has confirmed the validity of the compliance claim for the MAI.

Justification: independence enhances assurance credibility and addresses stakeholder confidence.

Evidence: ISA report which includes resolution of non-conformance or findings raised during the *independent safety assessment* process.

Evidence D2: Demonstration through objective evidence of compliance emanating from regulations and current best practice.

3.1.2 Concept of ‘Acceptably Safe’.

Requirements specific to the MAI, are still being established, particularly through the IMO’s development of the MASS Code [17]. As a result, this thesis adopts a goal-based approach to defining what constitutes ‘Acceptably Safe’. This is not a fallback for prescriptive compliance but an acceptable and defensible route where requirements are collaboratively derived by the relevant stakeholders and agreed upon with the relevant regulatory authorities. Formalising this definition is an important step in constructing a credible and defensible assurance/safety case for the MAI.

A review of existing literature across various domains, highlights how the notion of ‘Acceptably Safe’ is context dependent, and often determined by domain specific criteria. For example, the International Civil Aviation Organisation (ICAO) defines an Acceptable Level of Safety Performance as:

“The level of safety performance agreed by the State authorities to be achieved for the civil aviation system in a State” [69]

This emphasises the role of regulatory authorities in setting performance requirements. Similarly, ISO 21448, asserts that

“An acceptable level of safety for road vehicles requires the avoidance of unreasonable risk caused by every hazard associated with the intended functionality and its implementation, especially those not due to failures” [70].

Furthermore ISO 17894 states that

“The required level of safety shall be realized by appropriate activities throughout the lifecycle” [32]

which reinforces the necessity for lifecycle safety practices to be applied.

Leveson recommends a proactive approach that embeds safety considerations from the outset of system development, stating that the need to

“create techniques and approaches. that emphasise building safety into a system from the very beginning” [71].

From a regulatory perspective the Institute of Mechanical Engineers (IMechE) provides clear guidance on the principles of As Low As Reasonably Practicable (ALARP), which offers a structured framework to ensure the risks are reduced to a level that satisfied legal requirements [72]. Additionally, Osborne and Hawkins, describes that safety is context dependent’ reinforcing the need for domain specific requirements to be developed [73].

Drawing upon these diverse yet complimentary sources, it is evident that, safety cannot be defined in absolute terms for the MAI. Instead, safety must be articulated through stakeholder derived criteria based on their tolerability of risk. These criteria must be justified and integrated into the assurance/safety process to ensure that the MAI can be demonstrated as ‘Acceptably Safe’ within a defined context of use.

In conclusion and as illustrated in Figure 3-2, while the overarching safety objective (Goal G0) of ensuring that (X) is ‘Acceptably Safe’ to operate for a defined use case in a given environment applies equally to both conventional ships and the MAI, the assurance methodologies required to substantiate this claim differ substantially. For conventional vessels, assurance is achieved through compliance with existing prescriptive regulatory frameworks such as those found in SOLAS and related codes and conventions. Safety claims are substantiated through objective evidence demonstrating adherence to these regulatory requirements (D1), enabling the regulatory authorities to issue the necessary certificates for operation. This process is relatively straightforward as the deterministic nature or prescriptive regulations lends itself to clear verification procedures, but it does not involve the development of a safety argumentation process. While compliance with prescriptive requirements is necessary, it does not guarantee a claim of having a safe system.

In contrast, the assurance process for the MAI necessitates a more adaptive, stakeholder- driven and argument-based approach, as the regulatory landscape is still evolving and lacks substantive guidance. Consequently, the assurance evidence must be constructed through a systematic and iterative approach that involves the derivation of requirements (G4), the comprehensive identification and mitigation of hazards (G5), and demonstrable compliance with defined requirements, international standards, and applicable best practices (G6). This process is reinforced through an Independent Safety Assessment Process (ISAP) carried out by an Independent Safety Assessor (ISA) which adds a layer of credibility and helps to address stakeholder concerns.

The divergence between these two assurance pathways illustrates the challenges, complexity, and novelty of validating the assurance/safety argument for a socio-technical system such as the MAI. It also identifies the necessity for a multi-disciplinary and cross-sectoral engagement strategy to effectively manage the risks, especially where legacy regulatory frameworks are not yet equipped to address the complexities of the MAI. This divergence necessitates an evolving assurance/safety model that can accommodate the use of remotely controlled or autonomous functions within the maritime domain. Relying solely on compliance with prescriptive requirements, while necessary, does not guarantee that a system is 'Acceptably Safe'. Instead, it must be complemented by a structured safety argumentation process that explicitly articulates how the system, in its specific operational context, meets the safety objectives. Without such an argument, the assurance claim lacks the transparency, traceability, and contextual justification required to satisfy regulatory and stakeholder scrutiny.

3.2 Summary and transition to the MAI Lifecycle Process (LPM).

This chapter contrasts the conventional, prescriptively regulated approach to crewed ships with a goal-based assurance process for the demonstration of 'Acceptably Safe' in the context of the MAI. It identified MAI - specific risks, such as the loss of situational awareness, loss of connectivity, authority transfer, and the inability to isolate or reinstate autonomy, and emphasises that safety cannot be defined in absolute terms. Instead, safety must be articulated through stakeholder-derived, context-specific criteria agreed with competent authorities.

Given that provisions for the MAI are still being established, particularly through the IMO's work on a MASS Code and through individual flag state guidance, the analysis carried out within this chapter requires a shift from vessel-centric, prescriptive rule based compliance to a goal-based, argument-led approach that expresses safety as outcome-focused objectives and evidences them through a structured assurance/safety case rather than solely through rule based prescriptive compliance.

The LPM provides a process framework for managing context, change, and bias; the SPM structures the assurance argument and body of evidence; the LoP realises prevention, control, and recovery without reliance on immediate human intervention; and the MAI-DE specifies the boundary conditions within which each voyage-specific assurance case must be demonstrated. Taken together,

these elements constitute an acceptable and defensible approach to the demonstration of ‘Acceptably Safe’ for the MAI.

As shown in Figure 3-1, the MAI extends beyond the boundary of the vessel itself, which supports the thesis’s proposal to move from vessel-centric compliance to infrastructure level assurance. Acceptance is therefore contingent on the context of use and stakeholder requirements, which may change within a single voyage.

Chapter 4 introduces the design of the MAI Lifecycle Process Model (LPM), which serves as the process framework for the goal-based, argument-led assurance approach outlined in Chapter 3. The chapter begins by establishing a baseline for conventional crewed operations and then contrasts these with MAI operations. This comparison identifies where control, authority transfer, and assurance activities must be re-defined, across the vessel, Remote Operations Centres, connectivity solutions, and shore-side services. Next, Chapter 4 defines the requirements and design choices for a lifecycle process model that can adapt to changes in stakeholder requirements, jurisdictional conditions, and voyage or operational conditions. It also emphasises the importance of explicit acceptance criteria, independent assessment through an Independent Safety Assessment Process (ISAP), and traceable evidence.

This analysis provides the foundation for Chapter 5, which presents the LPM in detail (see Figure 5-1). Chapter 5 explains each element and its outputs, and demonstrates how the LPM integrates with the SPM, LoP, and the MAI-DE. Using this integrated framework, Chapter 5 translates the ‘Acceptably Safe’ objective into specific activities and verifiable outputs across the MAI lifecycle.

Chapter 4 : MAI Lifecycle Process Model (LPM).

This chapter serves as a critical link between the identification of assurance challenges in Chapter 3 and the detailed exposition of the Lifecycle Process Model (LPM) in Chapter 5. It introduces the rationale for, and overall structure of, the LPM, which is central to the thesis's approach to demonstrating that the Maritime Autonomous Infrastructure (MAI) can be considered 'Acceptably Safe' to operate in a defined context of use, and the development of the compelling body of evidence for regulatory review

As established in Chapter 3, the transition from conventional, crewed maritime operations to the Maritime Autonomous Infrastructure (MAI) introduces a range of novel challenges. These include the absence of harmonised regulatory frameworks, the complexity of distributed and cross-jurisdictional systems, and the need for continuous assurance across the entire operational lifecycle. Existing vessel-centric, prescriptive approaches are insufficient to address these challenges, particularly as the MAI encompasses not only the vessel but also remote operations centres, connectivity solutions, and a diverse set of stakeholders.

To address these gaps, this chapter introduces the Lifecycle Process Model (LPM): a structured, adaptive framework developed to support the systematic identification, management, and evidencing of safety for the MAI. The LPM is designed to form the basis of the claim of 'Acceptably Safe' operation in a defined context of use, providing the foundation for a compelling body of evidence suitable for regulatory review.

4.1 Rationale for Developing the LPM

The rationale for developing the LPM is based on the limitations of existing assurance methodologies. Without a structured, lifecycle-oriented process, there is a risk that emergent hazards, stakeholder requirements, and regulatory obligations will not be adequately identified or managed. The LPM was therefore developed to:

- Provide a systematic, repeatable process for identifying and managing risks across all phases of the MAI lifecycle.
- Enable stakeholder engagement and consensus-building by making requirements, tolerability of risk, and assurance activities explicit and traceable.
- Support the development of a defensible assurance/safety case that can adapt to evolving operational, technical, and regulatory contexts.
- Bridge the gap between high-level safety objectives and practical implementation, ensuring that assurance activities are both comprehensive and context sensitive.

4.2 Operational Cycle: Contrasting Conventional and Autonomous Operations

To contextualise the need for the LPM, it is important to establish the operational profile of a conventional crewed vessel. This profile has been compiled from the author's professional knowledge of the maritime sector, as well as a review of the operational characteristics of a vessel that is currently crewed, but is aiming to operate autonomously, such as the Yara Birkeland⁶.

The typical operational cycle for a conventional crewed vessel can broadly be categorised by a series of sequential phases, each involving distinct technical and procedural tasks. These phases commonly include:

⁶ Yara Birkeland: <https://gcaptain.com/yara-birkeland-worlds-first-autonomous-zero-emission-ship/> accessed on 2nd May 2025

Berthed in port⁷ – loading cargo – ballast – making vessel seaworthy - leaving the berth under pilotage – under-way, manoeuvring – following the agreed voyage plan and making way - anchoring⁹ – pilotage to the berth – berthed in port – unloading cargo – ballast – bunkering or charging power sources – replenishment of consumables – water, oil, food, spares – removal of waste products – facilitating inspection by the relevant authorities – providing the required information for arrival and departure – facilitating repair and maintenance personnel on board and disabled¹⁰ and drifting¹¹ as potential operational scenarios.

Where a change in the voyage plan, voyage conditions, or operational conditions occur, the risks associated with the change are managed by the crew and master on board the vessel. Where the vessel is operating with no crew on board, all phases of the operational cycle will need to be either controlled by a remote operator, or through the technologies on board the vessel that support autonomous operations.

Several of the phases within the operational cycle present significant challenges for the MAI if there are no crew on board. Examples include verifying the vessel's seaworthiness throughout the voyage, or ensuring cargo is loaded and unloaded without overstressing the hull structure or exceeding the vessel's stability limits. These complex tasks which require precise operational control, which are traditionally executed and supervised by onboard personnel, may now be carried out through remotely controlled systems or autonomous functions within a defined safety assurance/safety process as developed within this thesis.

Additionally, facilitating inspection by the relevant authorities or repair and maintenance activities will need to consider the risks associated with remote or autonomous isolation of a function. An example of which is isolation or control of an electrically driven essential services pump:

⁷ (verb) to bring a ship to a berth. (noun) the wharf space at which a ship docks. A wharf may have two or three berths.

⁸ Port as any port, terminal, offshore terminal, ship and repair yard or roadstead which is normally used for the loading, unloading, repair and anchoring of ships, or any other place a ship can call.

⁹ Anchoring is a process that secures the vessel to the bed of a body of water to prevent the vessel from drifting due to wind or current.

¹⁰ Disabled is defined as a vessel damaged or impaired in such a manner as to be incapable of proceeding on its voyage.

¹¹ Drifting is defined as 'being driven along by the wind, tide or current'

- **Crewed vessel** – crew or service engineer can manually isolate the pump and initiate local starting and stopping.
- **Uncrewed vessel** – remotely controlled pump functions: crew or service engineer attending on-board can manually isolate the pump and initiate local starting or stopping. Where the start/stop is initiated from a remote operator, all relevant stakeholders must be immediately informed if there is a loss of connectivity between the vessel and the remote operator to ensure the risks do not become intolerable.
- **Uncrewed vessel** – autonomous operation of the pump functions: crew or service engineer attending on board may be able to isolate the pump and initiate local starting or stopping. Where the start/stop is initiated by the autonomous system, verification that the autonomous system is isolated must be immediately available to all relevant stakeholders to ensure the risks do not become intolerable. The processes for reinstatement of the autonomous function will also need to be defined and agreed upon by all relevant stakeholders.

In the absence of an onboard crew, safety-critical actions that were once manual and immediate now require clear procedural safeguards, real-time status verification, and robust communication protocols between autonomous systems, remote operators, and attending personnel. Additionally, broader system-level considerations must extend to shore-based elements of the MAI, including inspections by regulatory or security authorities and the management of supporting non-marine facilities. These interactions directly influence the overall assurance/safety case and the validity of the ‘Acceptably Safe’ claim for a given voyage.

To address these challenges, the following chapter introduces the Lifecycle Process Model (LPM), outlining its structure, the interdependencies between its phases, and its integration with the MAI Design Envelope (MAI-DE), the Safety Process Model (SPM), and the Layers of Protection (LoP). Together, these models form a comprehensive framework for supporting assurance activities within the MAI context.

4.3 Development and Structure of the LPM

Developed through a combination of critical literature review, analysis of regulatory and industrial best practice, and engagement with technical and academic experts, the LPM is structured to reflect the need for adaptability, traceability, and stakeholder inclusivity, and comprises a series of sequential and iterative phases, each corresponding to a key stage in the lifecycle of the MAI. These include:

- **Goal and Concept Definition:** Establishing clear objectives, stakeholder requirements, and the intended operational context.
- **Hazard and Risk Analysis:** Systematically identifying hazards, evaluating risks, and defining tolerability thresholds.
- **Design and Implementation:** Embedding inherently safe design principles, fault tolerance, and layers of protection.
- **Verification and Validation:** Ensuring that safety requirements are met through testing, simulation, and independent assessment.
- **Operation, Maintenance, and Disposal:** Managing risks during routine operation, maintenance, and eventual decommissioning, including the management of change and personnel transitions.

Each phase is supported by structured decision points (stage gates), predefined acceptance criteria, and mechanisms for independent challenge and evidence traceability.

4.4 Integration with Supporting Models

The LPM does not operate in isolation. It is integrated with three supporting models developed within this research:

- **Safety Process Model (SPM):** Provides a structured methodology for deriving safety requirements, verifying compliance, and consolidating evidence.
- **Layers of Protection (LoP):** Introduces independent barriers to prevent, control, and mitigate faults, compensating for the absence of onboard crew.
- **MAI Design Envelope (MAI-DE):** Defines the operational safety boundary, mapping layers of protection against voyage and operational conditions.

Together, these models form a comprehensive assurance framework, enabling the systematic identification and management of risks, supporting stakeholder engagement, and facilitating regulatory acceptance.

4.5 Significance and Contribution of the LPM

The LPM represents a novel and essential contribution to the assurance of maritime autonomy. Its significance lies in;

- **Enabling dynamic, context-sensitive assurance:** The LPM accommodates changes in operational conditions, stakeholder requirements, and regulatory expectations, ensuring that assurance activities remain relevant and robust throughout the MAI lifecycle.
- **Supporting the ‘Acceptably Safe’ claim:** By providing a structured process for hazard identification, risk management, and evidence generation, the LPM forms the basis of a compelling assurance/safety case for regulatory review.
- **Facilitating cross-stakeholder engagement:** The LPM makes requirements, responsibilities, and tolerability of risk explicit, supporting consensus-building and transparent decision-making.
- **Advancing the state of the art:** Unlike existing vessel-centric frameworks, the LPM addresses the unique challenges of the MAI as a distributed, socio-technical system-of-systems.

The LPM provides a comprehensive and flexible framework for managing safety assurance within the MAI. Its structured approach enables stakeholders to identify, evaluate, and address risks in a transparent and consistent manner, supporting the ongoing development of credible and defensible assurance/safety cases as the operational and regulatory landscape continues to evolve.

4.6 Transition to Chapter 5

While this chapter has introduced the rationale, development, and high-level structure of the LPM, Chapter 5 provides a detailed breakdown of each element, illustrating how the LPM integrates with the SPM, LoP, and MAI-DE to support the systematic development of a compelling assurance/safety case. Practical examples and case studies will demonstrate the application of the LPM in representative MAI scenarios.

Chapter 5 : MAI Lifecycle Process Model (LPM).

The proposed Lifecycle Process Model (LPM) as illustrated in Figure 5-1, builds upon established standards and good practices such as those defined in [30] [32] [37] [39] [70] [74] [75][76]. It provides a systematic framework for identifying the elements of the MAI that are important to safety and establishes a methodology that provides a structured, coherent, and traceable decision-making process. This process is fundamental to safety assurance and to the development of the compelling body of evidence that demonstrates the MAI is 'Acceptably Safe' within its defined context of use.

Although the LPM is presented as a structured linear framework, it is designed to be inherently adaptive and iterative. This adaptability is essential for continuous assessment and refinement as operational conditions change, such as alterations to the vessel's port of arrival or the unexpected loss of connectivity on the planned route, which can have an impact on control of the vessel's functions. Consequently, the LPM accommodates the dynamic and evolving safety assurance process, changing regulatory requirements, jurisdictional differences and the complexities when transitioning between voyage or operational conditions.

Furthermore, the application of the LPM necessitated a context-specific approach, as each project is anticipated to generate a distinct set of requirements, shaped by the risk tolerability thresholds, stakeholder requirements, and regulatory obligations. For example, port authorities may impose specific operational restrictions on the operation of MAIs within their jurisdiction, or require external support, such as tug assistance, during berthing and unberthing or even prohibit autonomous operations entirely. Similarly, pilotage requirements may require a clearly defined communication framework and declaration of predefined fallback states before vessels of this type are permitted entry.

The LPM's structured approach supports the development of:

'a compelling body of evidence that without bias, makes a claim for both the 'safe and unsafe' characteristics of a system when used for a defined use case in a given environment'. SCSC-159 [77].

A compelling body of evidence refers to a structured, traceable, and comprehensive set of data, analysis, and justifications that collectively substantiate the claims regarding the safety and operation of the MAI within a defined context of use. Such evidence should include, but not limited to, the outcome of hazard identification, structured risk assessments, verification and validation results derived from simulations and testing, documented evidence demonstrating compliance with identified standards and regulatory requirements, and a clearly articulated design rationale linking system requirements to the implemented safety functions [78] [79].

For conventional vessels, what constitutes sufficient and relevant evidence is defined by the prescriptive requirements of the regulations and, where applicable, classification society rules. In contrast, due to the absence of prescriptive regulations and divergence of regulatory and classification requirements, the evidence to be submitted for MAI regulatory review must be derived and defined through consensus among the relevant stakeholders. While there is no explicit regulatory requirement that this evidence is presented without bias, an assurance/safety case built on biased evidence may not withstand scrutiny and could fail to demonstrate that the MAI is 'Acceptably Safe' to operate in a defined context of use. Consequently, a commitment to objectivity, transparency, and intellectual integrity in the development of the assurance/safety case where both negative and positive findings are disclosed is essential [80].

This principle is further reinforced by the Safety Critical Systems Club (SCSC) in their document Assurance Case Guidance 2021 [77] which identifies the need to:

‘create well-balanced arguments that seek out positive (affirming) and negative (non-affirming) evidence with equal vigour’ and the ‘necessity to overcome the more personal and often completely unintentional biases that could continue to restrict the development of well-balanced assurance cases – the cognitive biases’.

Within the context of the MAI, the influence of cognitive bias may be further amplified due to two key factors: the prevailing reliance on traditional shipbuilding processes and the limited operational experience in remote control or autonomous vessel functions. These conditions can lead to the inadvertent transfer of legacy assumptions into the assurance/safety arguments for the MAI, which can impact the evidence required to support the requirement of an ‘Acceptably Safe’ MAI.

5.1 Controlling Bias




Controlling cognitive and institutional biases is therefore essential for maintaining the integrity of the assurance/safety case. This requires stakeholders to critically evaluate the relevance and sufficiency of all supporting evidence, particularly when that evidence originates from conventional practices that may not be applicable to remotely controlled or autonomous operations of the MAI.

An example of such bias is the uncritical acceptance of certificates issued by a classification society without analysing how their certificates support the assurance/safety argument. Noting that classification societies are not guarantors of safety, their certificates must be evaluated against the assurance/safety case requirements as they may not provide sufficient evidence that the unique risks associated with autonomous or remotely controlled functions have been adequately addressed. Therefore, assurance/safety case practitioners must resist the temptation to equate certification with safety, and evaluate each certificate against the specific claims, evidence and arguments within the LPM.

A further example of cognitive bias is the reliance on past experience as a justification for safety assurance. For example, the acceptance of a product may be based on its extensive use in conventional, crewed maritime operations. Yet, such experiential evidence may not be directly transferable to crewless vessels, as performance proven in crewed context does not guarantee safe operation on crewless vessels. This can lead to unfounded confidence in system performance under fundamentally different conditions.

Given the limited operational experience and empirical data available for remote control or autonomous functions, coupled with the shift in responsibility from onboard personnel to remote operators and system designers, such assumptions introduce substantial risks. This enforces the need for independent scrutiny and validation. Accordingly, the involvement of an ***independent safety assessor*** (ISA), a professional responsible for challenging the assurance/safety case, becomes a key measure in mitigating the effects of cognitive bias. The ISA's role includes evaluating the assumptions, verifying the completeness and quality of evidence, and ensuring the assurance/safety case is supported by robust, objective evidence.

In summary, recognising and addressing cognitive bias is essential to the credibility of the assurance/safety argument for the MAI. Without the input of the ISA, the assurance/safety case may inadvertently become an exercise in confidence rather than an objective demonstration of safety, making the claim of 'Acceptably Safe' challenging to substantiate. Furthermore, this thesis also recognises the need for a formal ***independent safety assessment process*** (ISAP) that is distinct from the individual ISA's role. This process provides a structured, repeatable mechanism to validate the assurance/safety case throughout the MAI lifecycle.

- Note 1: Stage Gates will be defined and agreed by relevant stakeholders.
- Note 2: Disposal as described in 5.2.14 and illustrated as 'A' refers to the withdrawal, decommissioning, or replacement of hardware and software elements. Where changes involve personnel, such transitions are treated as part of organisational change management rather than disposal and require assurance that incoming staff are suitably qualified and experienced (SQEP) for their assigned roles.
- Note 3: The Operate Maintain Diagnose Repair (OMDR) described in 5.2.13 and illustrated as 'B' shall satisfy the requirements from the stakeholder analysis.
- Note 4: Where dynamic stakeholder requirements occur, the risk(s) are to be evaluated to ensure the claim of 'Acceptably Safe' can be achieved.
- Note 5: Influences - the flow through the SPM and informs, rather than determines, the justification structure of the final safety case claims
-  Impacts on – informational dependency: supplies evidence/ context to elements of the SPM. 
- Note 6: LPM Stages included within the MAI-DE (Fig 5-5). 

As illustrated in Figure 5-2, the elements of the MAI, exist within a network of reciprocal relationships within which element can influence or be impacted on by other elements.

Influences occur when one element shapes or constrains the parameters, requirements, or decision-making processes of another. For example, the Stakeholder Requirements influence the Assurance/Safety Case by determining the evidence needed to substantiate the safety claims.

Impact on represents consequential effects where changes in one element alter the condition of another, for instance, the Voyage Condition can impact on the Operational Conditions by requiring the involvement of human operators.

The number and positioning of stage gates will be determined by the relevant stakeholders based on factors such as the tolerability of risk or changes in the overall project goal, which may necessitate the re-evaluation of previous or upcoming stages of the LPM. The application of the stage gate process is further illustrated in Section 6.

5.2 Elements of the LPM explained.

The preceding section establishes that uncontrolled biases can erode the credibility of an assurance/safety case. The LPM (Figure 5-1) is designed to counter those biases by imposing structured decision points, predefined acceptance criteria, independent challenge, and evidence traceability from concept through disposal. This section explains how the LPM translates high-level safety requirements, such as inherently safe design and the claim of “Acceptably Safe” into actionable tasks and verifiable outputs. Each activity is defined not only by its technical role but also its contribution to bias control. For example, the LPM requires explicit claims and fallback states, separates hazard identification from risk evaluation, mandates independent verification, and ensuring that per-voyage updates refresh the evidence base rather than relying on unexamined precedent. In this way, the LPM systematically embeds checks and balances throughout the assurance process, strengthening the credibility and transparency of the assurance/safety case.

5.2.1 Goal

The ‘Goal’ for the MAI will be derived and defined by the company, owners, and relevant stakeholders, and must incorporate overarching requirements related to safety, environmental protection, security, technical performance, and financial constraints. It should be sufficiently precise to eliminate ambiguity and prevent divergent interpretations among stakeholders. At the same time, it must be adaptable to accommodate changes in laws, regulations, technological advancements, emergent risks, and evolving business needs as they arise throughout the project lifecycle. To ensure clarity, these requirements shall be expressed in clear, measurable and actionable terms, to include the principles of inherently safe design, and fault tolerance, as described in section 5.5.2.1. As examples, these can be expressed as:

- *Ensuring the timely and efficient delivery of cargo on time, between Port A and Port B.*

- *Preventing single points of failure that could lead to a complete loss of a function – examples, complete loss of thrust or steering.*
- *Maintaining compliance with all applicable regulatory requirements.*

Although the ‘Goal’ for the MAI is defined internally by the company, vessel owners, and other relevant stakeholders, it is heavily influenced by external factors such as regulatory obligations, environmental standards, and market or operational expectations. As such, the goal must balance internal priorities with external demands to ensure feasibility, compliance, and long-term viability of the MAI.

5.2.2 Concept.

Building on the defined project goal, the ‘Concept’ phase of the MAI must establish clear and well-defined high-level objectives that are informed by a diverse range of requirements, including but not limited to the:

- specific applications and intended use of the MAI, which will directly influence the system architecture and safety requirements.
- geographical, environmental, and route specific factors that may influence the operational feasibility of the planned voyage. These can include weather conditions, ice coverage, anticipated temperature, and connectivity coverage.
- operational conditions for the voyage, including whether the vessel will be crewed or uncrewed at different stages of the voyage. For example: a vessel may be autonomous in open water but require human intervention in port or congested waters. Defining these transition points and ensuring seamless operational control across the different phases is essential.

- legal and regulatory obligations from the flag-state, as well as non-statutory requirements such as compliance with International Standards and, where applicable, classification society requirements.
- tolerability of risk shall be defined and agreed upon by the relevant stakeholders at the start of a project as it will inform the complete lifecycle of the MAI. In this context, the definition of ‘tolerable risk’ has been adapted from ISO/IEC Guide 51:2014, Definition 3.15 [81], which is the risk that is :
 - *‘acceptable in a given context based on current values of society’* which has been adapted for this thesis to the:
 - *‘ acceptable in a given context based on the current requirements of the relevant stakeholders’.*

As an example, shipowner A - may consider a constructive total loss and sinking of a vessel as a tolerable risk; however, shipowner B may consider it to be intolerable as the costs associated with the recovery of the vessel and potential environmental damage fines could be substantial. The vessel operated by shipowner A is a 4.5m survey vessel, battery-powered, operating autonomously and in coastal waters. If the vessel sinks, the owners can recover it using divers. The vessel operated by shipowner B is a 3500-ton container ship operating in coastal waters; however, the ship could pose a significant risk to the environment and operation of the port if it sank in the entrance to the port. The determination of **‘tolerable risk’** is a decision for the relevant stakeholders to address.

By systematically addressing these requirements, the MAI concept phase ensures that the infrastructure is developed within a structured framework, capable of adapting to the safety assurance needs of the MAI within a complex and evolving technological, regulatory, and operational environment, along with shifting stakeholder requirements

5.2.2.1 Inherently Safe Design.

This section examines the principle of inherently safe design and its application within the MAI. Widely adopted in the nuclear and process engineering sectors, it prioritises the elimination of hazards at the design stage rather than relying on procedural controls or reactive mitigation. Its relevance to the MAI lies in the absence of onboard trained personnel who have historically served as a layer of protection capable of identifying, interpreting, and responding to emerging failures before they escalate into intolerable risks.

In the context of the MAI, a lack of human intervention requires a fundamental shift from a compliance driven design towards a risk informed design that requires hazard elimination over hazard control, and design philosophies that prioritise inherent safety. This represents a fundamental transformation in maritime safety thinking, one that is not yet widely recognised in existing regulatory requirements but essential for the successful introduction of maritime autonomy and remotely operated vessel functions.

This thesis proposes the adoption of inherently safe design principles within the MAI development, thereby making a unique contribution to this thesis. It advances the argument that safety cannot be achieved by simply substituting human oversight with automation or remote control; rather safety requirements must be embedded into the design of the MAI from the outset. This shift in design philosophy is not only necessary, but foundational to supporting the ‘Acceptably Safe’ claim under dynamic regulatory and operational conditions.

The objective of an inherently safe design is to reduce the number of events that result in a loss or degradation of a function below acceptable levels. As stated by Kletz T in his 1978 article: ***‘What you don’t have can’t leak’ - ‘before we estimate the probability and consequence of a hazard and compare them with a target, we should ask if the hazard can be eliminated’*** [82]. Which supports the principle that the most effective risk control is hazard elimination.

A similar principle is used by the Office for Nuclear Regulations in their document Safety Assessment Principles for Nuclear Facilities:2014 Edition, Revision 1 (January 2020) [83] states:

“The underpinning safety aim for any nuclear facility should be an inherently safe design, consistent with the operational purposes of the facility. An ‘inherently safe design’ is one that avoids radiological hazards rather than controlling them. It prevents a specific harm occurring by using an approach, design or arrangement which ensures that the harm cannot happen”

Likewise, the UK Health and Safety Executive document ‘Reducing Risks, Protecting People’ [84] advocates the principle of an *Inherently safer design*:

“Adoption of the principles of inherently safer design is particularly important where the consequences of plant or system failure are high. HSE will press for the incorporation of inherently safer design features, where these are possible, to reduce the reliance on engineered safety systems or operational procedures, to control risk”

Where it is not reasonably practicable to achieve an inherently safe design, the MAI must demonstrate *fault tolerance* which is defined by the IEC [39] as:

“the ability of a function to continue to perform in the presence of a fault”

The application of the inherently safe design principle is particularly relevant for the MAI, as the layer of protection afforded by the onboard crew will no longer be available on a crewless vessel. To contextualise this principle, Table 5-1 presents a tailored adaptation of the safety principles published by the ONR to reflect the operational and regulatory characteristics of the MAI. These tailored principles emphasise the necessity of clearly defining operational conditions and statutory requirements at the outset of the MAI development and maintained throughout its lifecycle.

ONR Principle	MAI Adapted Principle
Underpinning safety aim for any nuclear facility should be an inherently safe design, consistent with the operational purposes of the facility.	The underpinning safety aim for the MAI should be an inherently safe design consistent with (all) defined operational and statutory requirements.
An ‘inherently safe’ design is one that avoids radiological hazards rather than controlling them. It prevents a specific harm occurring by using an approach, design or arrangement which ensures that the harm cannot happen. Inherent safety is not the same as passive safety. When an inherently safe design is not achievable. The design should be fault tolerant.	An ‘inherently safe’ design is one that <u>avoids hazards</u> rather than controlling them. It prevents a specific harm occurring by using an approach, design or arrangement which ensures that the harm cannot happen. Inherent safety is not the same as passive safety. When an inherently safe design is not achievable. The design should be fault tolerant.
Fault Tolerance – The sensitivity of the facility to potential faults should be minimised.	Fault Tolerance – ability of a function to continue to perform in presence of a fault [39]

Table 5-1: Adaption of the ONR Safety Principles for application to the MAI

5.2.2.2 Challenges in Application of Inherently Safe & Fault Tolerant Design within MAI

While inherently safe design offers a powerful approach to risk reduction in the MAI, its practical implementation faces several significant challenges:

- **Skills and Competency Gaps** - The maritime sector is undergoing rapid technological transformation, but there is a well-documented shortage of personnel with the expertise required to design, assess, and operate inherently safe autonomous systems [134][135]. Traditional maritime training has focused on operational safety and compliance, rather than proactive hazard elimination or advanced risk modelling. As a result, there is a pressing need for upskilling and continuous professional development, particularly in areas such as systems engineering, digital safety, and AI-driven risk assessment.
- **Complexity and Interdependencies** - The MAI is a system-of-systems, often relying on technologies outside the traditional maritime domain, such as space-based connectivity (satellite communications), advanced sensors, and remote operations centres. Conducting comprehensive risk assessments across all elements, including those provided by third parties or external sectors can be extremely challenging. For example, the reliability and security of

satellite links may be critical for safe vessel operation but are outside the direct control or expertise of maritime stakeholders.

- **Limitations of Hazard Elimination**- Not all hazards can be eliminated at the design stage, especially in complex, interconnected systems such as found within the MAI. Some risks may only be mitigated or controlled, requiring robust fault tolerance and fallback strategies. For instance, emergent behaviours in AI systems may introduce new risk patterns that are difficult to foresee or fully eliminate.
- **Regulatory Barriers** - Existing maritime regulations are built around crewed operations and are largely prescriptive, vessel-centric, and do not support or recognise the principles of an inherently safe design at a SoS level. The regulatory and jurisdictional requirements to address this are outside the scope of this thesis, however, a failure to address this could hinder the adoption of maritime autonomy for international voyages and complicate certification and regulatory approval processes.
- **Human Oversight** – The IMO is requiring human oversight even in autonomous operations this ensures that accountability is preserved throughout operational scenarios. Designing for inherent safety must account for limitations and capabilities of the remote operators, where the allocation of function between the operator and the technology under normal, RFAE and emergency conditions must be considered. To support effective human interaction, clear user interfaces and robust decision support tools should be integrated from the earliest stages of project development. Embedding Human-Centred Design principles [140] ensures that remote operators can interact confidently and efficiently with complex technologies as found within the MAI.
- **Resources and Cost Constraints** - Developing and implementing inherently safe systems often requires significant investment in new technologies, training, and assurance processes. High upfront costs and uncertainty about return on investment may deter operators and shipowners from adopting these approaches, especially in a competitive market.

The transition to inherently safe design within the MAI is both necessary and challenging. Overcoming these barriers will require coordinated efforts in workforce development, cross-sector collaboration, regulatory reform, and ongoing research into risk assessment methodologies that can accommodate the complexity and evolving nature of autonomous maritime systems. Only by meeting these challenges can the sector fully realise the benefits of ‘Safe by Design’ and ensure the robust, resilient operation of future maritime infrastructure.

To illustrate these challenges and the practical implications of adopting inherently safe design within the MAI, the following case studies are presented. Table 5-2 – namely an electrical fault and a fuel oil leak, represent reasonably foreseeable abnormal events (RFAE) within the context of the MAI. Each scenario is analysed across three vessel configurations: crewed, remotely controlled functions, and fully autonomous. This comparative analysis illustrates the evolving allocation of the safety responsibilities required for each configuration as human presence is reduced or eliminated.

In conventional maritime operations, trained onboard crew are responsible for both incident response and the identification of root cause analysis and hazard elimination, as required by the STCW Code Pt A Ch III [87]. In contrast, autonomous or remotely controlled operations, these responsibilities shift significantly. The competencies and decision-making capabilities traditionally held by the crew must instead be embedded within the system’s design architecture and operational logic from the earliest stages of development. This transition reflects a broader redistribution of accountability, wherein the obligation to demonstrate that the MAI is ‘Acceptably Safe’ is transferred from the vessel’s crew to system designers, developers, and remote operators.

As shown in Table 5-2, the first case study involving a circuit breaker tripping due to overload, raises questions regarding design alternatives. For example, could mechanical circuit breakers be replaced with solid-state switching devices? This would remove the mechanical failure mode altogether, aligning directly with the principle of hazard elimination that underpins Inherently Safe Design. Furthermore, where legal restrictions prevent ROC operators from resetting equipment located in land-based installations, time becomes a safety-critical variable, which could be substantially longer than observed on a crewed vessel. This dependency on external personnel to restore a lost function must be explicitly modelled within the LPM, as it may have an impact on safety of the MAI.

By contrast, the second case study of a fuel oil leak, presents heightened risk under remote or autonomous control due to the absence of crew for immediate containment or cleanup. This raises a fundamental design question: is fuel oil a necessary component of the MAI? If not, its elimination would remove the hazard at source, satisfying the Inherently Safe Design criteria.

Overall, these scenarios reinforce the core proposition that inherently safe design is not an optional enhancement but a foundational requirement for the successful implementation of the MAI. The lessons drawn from these case studies illustrate that traditional crew-based risk management strategies cannot simply be substituted with remote or autonomous systems; rather, safety must be systematically embedded into the MAI from the earliest design stages. This transformation in safety thinking is essential not only to meet the operational challenges of the MAI but also to support the broader regulatory and stakeholder acceptance of 'Acceptably Safe' claims in the evolving maritime domain.

Table 5.2 - Inherently Safe Design and Fault Tolerant Design examples:			
Event	Crewed Vessel	Remotely Controlled Function - Crewless	Fully Autonomous Function – Crewless Inherently Safe Design
Circuit breaker tripping due to overload or short circuit, could result in loss of function. To restore function, the overload or short circuit condition would need to be identified, isolated & rectified allowing circuit breaker to be reset.	STCW-trained crew will identify the fault, isolate, rectify and restore the function – Time is an attribute of safety needs to be considered when restoring the function.	<p>If circuit breaker is on board, it may be difficult to rectify fault remotely. Arrangements should be made to supply the function through alternative means. Where circuit breakers are remotely closed, compliance with ICu/ICs ratings of breakers needs to be considered. If the circuit breaker is within the ROC, there may be requirements to have land-based qualified personnel available to reset the breaker. Time as an attribute of safety maybe considerably longer than on a crewed vessel if there is reliance on external specialists to restore the function.</p> <p>Requires further analysis within the design process</p>	If circuit breaker is located on board the vessel it may be difficult to rectify the fault remotely as physical intervention maybe required to identify and resolve the issues. Could the system be designed without circuit breakers, solid state switching?

Table 5.2 - Inherently Safe Design and Fault Tolerant Design examples:			
Event	Crewed Vessel	Remotely Controlled Function - Crewless	Fully Autonomous Function – Crewless Inherently Safe Design
A fuel oil leak could result in an explosive gas atmosphere occurring and a hazard to personnel	Onboard crew can isolate leak, rectify fault, ventilate the space & clean the area to prevent an accident occurring to humans (slips, trips and falls) or damage to environment.	Means to remotely isolate the fuel oil leak should be provided along with means to gas free the space and verify that it is not an explosive gas atmosphere. This requires suitable positioned sensors, cameras and verification processes in place etc. The oil spill will have to wait until authorised and competent personnel board the vessel to clean the space and rectify the failure. Requires further analysis within the design process	The necessity of fuel oil as an energy source should be evaluated as part of hazard elimination
See Figure 5-1 –Overall safety requirements, Fallback state, Layers of Protection, Hazard and risk analysis, Tolerability of risk, Overall safety validation.			

Table 5-2: Inherently Safe Design and Fault Tolerant Design examples for Crewed and Crewless operations

As illustrated in Figure 5-3 below, the implementation of inherently safe and fault-tolerant design begins with the systematic identification of all elements of the MAI. This identification will be informed by the specific voyage and operational conditions and incorporates a hazard and risk analysis that involves all relevant stakeholders.

Any gaps in this process could undermine the ability to demonstrate that risks do not become intolerable throughout the lifecycle of the MAI. Furthermore, where changes occur within a single voyage, the assurance/safety case must be treated as a continuous and adaptive process. This ensures that risks are continuously reassessed and controlled, rather than being treated as static elements [85].

Given the complexity of the MAI, this process must be supported by an independent safety assessment carried out by an ISA. Further details on this requirement are provided in Section 5.2.8, Hazard and Risk Analysis.

Although Figure 5-3 focuses specifically on the principles of inherently safe and fault-tolerant design, it forms a logical foundation for expansion through the integration of the LoP framework. The LoP concept builds on this initial assessment by introducing structured layers of protection strategies that complement inherent safety with engineering safeguards, procedural controls, and organisational measures. When applied together, inherently safe design, fault tolerance, and layered protection form a comprehensive and hierarchical approach to risk reduction within the MAI, ensuring the absence of on-board crew does not equate to the absence of safety.

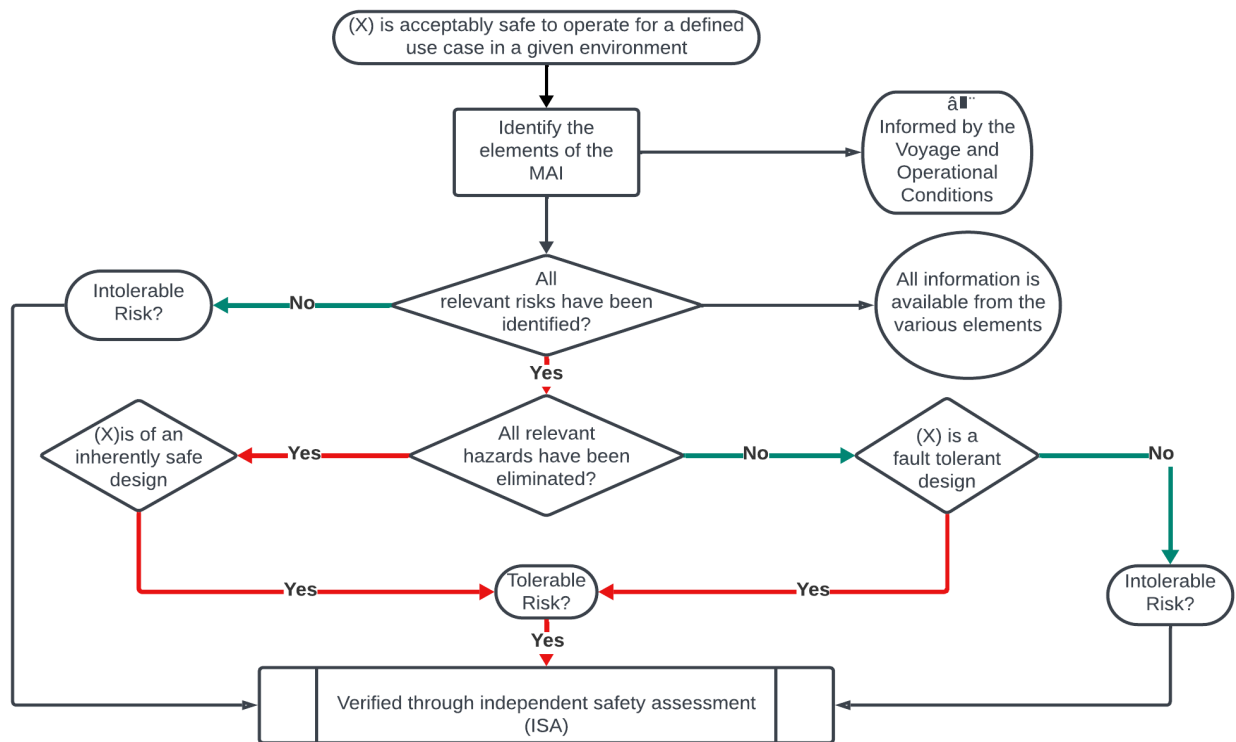


Figure 5-3: Inherently Safe Design and Fault Tolerant Assessment Model

5.2.3 Voyage Plan.

Voyage planning is a complex operation and is considered of ‘*essential importance for safety of life at sea, safety and efficiency of navigation and protection of the marine environment*’ as defined by the IMO Resolution A 893(21) [86]. This resolution, titled Guidelines for Voyage Planning, states that voyage planning applies to all vessels. Section 2 of A.893(21) (2.1.9) – Appraisal; provides a comprehensive list of items to be taken into consideration in voyage and passage planning including:

‘Any particular items pertinent to the type of the vessel or its cargo, the particular areas where the vessel will traverse, and the type of voyage or passage to be undertaken’.

In addition, voyage planning is a requirement under Section A-VIII/2 Part 2.3 of the International Maritime Organisation – International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW) [87]:

“the voyage to be planned in advance taking into account pertinent information and any course laid down shall be checked before the voyage commences”.

It further identifies the responsibilities of the master in regards planning as follows: :

“[The master must] consider whether any particular circumstance, such as the forecast of restricted visibility in an area where position fixing by visual means at a critical point is an essential feature of the voyage or passage plan, introduces an unacceptable hazard to the safe conduct of the passage; and thus, whether that section of the passage should be attempted under the conditions prevailing or likely to prevail. This could include environmental conditions such as snow, fog, rainfall, illumination, wind, and sea state”.

Additional operational considerations arise when the vessel or vessel function(s) are designed to be remotely controlled from a ROC located off the vessel. Any known limitations or potential degradation of the connectivity service between the ROC and the vessel must be evaluated and included into the voyage plan, especially if the loss or degradation could have an impact on the safe conduct of passage. Furthermore, a degradation of the technology that supports situational awareness, such as salt deposits or snow/ice on the lens of a camera must also be considered. These requirements introduce distinct operational considerations, setting the MAI apart from conventional vessel operations.

In certain circumstances, the master may be required to abandon the voyage plan. In such cases, where this occurs, IMO Res A 893(21) 3.2.2.9 requires that:

“Contingency plans for alternative actions to place the vessel in deep water or proceed to a port of refuge or safe anchorage in the event of any emergency necessitating abandonment of the plan, considering existing shore-based emergency response arrangements and equipment and the nature of the cargo and of the emergency itself”.

For the MAI, the contingency plan will need to be derived, potentially diverging from the guidance given in IMO Res A 893(21). For example, the vessel may not be fitted with anchoring equipment (see

Section 6.1.2), or there may be insufficient power to place the vessel in deep water. These deviations need to be considered within the LPM. A key consideration will be the extent to which the MAI itself is responsible for implementing the contingency plan, or whether control will transfer to a human (whether on-board the vessel or remotely). Upon initiation of a contingency plan, it is essential that all relevant stakeholders and actors are promptly notified, with verification of communication conducted by appropriate means.

5.2.4 Stakeholder and Actor Analysis.

As shown in Figure 5-1, the Stakeholder and Actor Analysis instantiate the stakeholder layer of the MAI for the current concept/voyage. It takes inputs from the 'Goal', 'Concept' and 'Voyage Plan', and produces a set of requirements that influence and informs the SPM by setting acceptance criteria that are informed by technical, legal or operational requirements.

The operation and assurance of the MAI involve a complex interplay of entities with different roles, interests, and influences. In analysing these roles, it is important to distinguish between '**actors**' and '**stakeholders**', as each has a unique relationship with the MAI's safety, performance, and regulatory compliance.

Within the MAI, '**actors**'¹² are defined as entities—human or non-human—that directly interact with or influence the operational functions and performance of the MAI. This includes onboard or offboard technical systems that perform automated functions (such as situational awareness algorithms or search and rescue), as well as human operators in Remote Operations Centres (ROC), pilots, and external operational entities such as tug operators. Actors are therefore the active agents of change and control within the operational framework of the MAI.

By contrast, '**stakeholders**' encompass all parties who have an interest in, or are affected by, the MAI's operations, irrespective of whether they directly interact with the system. Stakeholders include not only actors (e.g., ROC operators and onboard crew) but also those who establish regulatory and safety

¹² In Table 5-3, the actors relevant to this analysis are denoted in orange within the column labelled 'Actors/Stakeholder.'

expectations, economic interests, or social impacts, such as regulators, classification societies, insurers, cargo owners, coastal communities, and environmental groups.

Understanding this distinction is critical to ensuring a comprehensive and credible safety assurance process. While actors directly affect operational functions and fallback states, stakeholders influence the **'requirements for safety'** and the **'acceptability of risk'** which in turn influence the evaluation of 'Acceptably Safe' within the regulatory and operational context

As the MAI introduces new actors into the operational domain and creates novel challenges in stakeholder engagement, it becomes imperative to ensure accurate identification and categorisation of stakeholder relationships. It is essential to capture the unique requirements of each stakeholder and foster transparent dialogue within a common operational framework.

Stakeholder engagement is therefore a critical process in supporting the successful integration of the MAI within the maritime industry. This stakeholder analysis provides a foundational framework for understanding the diverse stakeholder roles and requirements that need to be considered, to facilitate effective MAI integration within existing maritime systems.

The maritime industry has an established set of stakeholders but, the innovative nature of the MAI introduces new stakeholders, which includes land-based regulators, land-based remote operators, off-ship maintenance providers, data analysts, land-based emergency services and emerging technology developers. Established stakeholders such as fuel suppliers, port authorities, and insurers, may be faced with evolving requirements. For example, who has the authority to sign for the fuel and ensure the correct amount of the right quality has been delivered and with whom do the port authorities and security services communicate with if the vessel is crewless? Each stakeholder has a distinct responsibility that can directly influence the safety and regulatory acceptability of the MAI and must therefore be systematically considered within the LPM. For example, insufficient fuel for the voyage or physical security alerts could have an impact on the safety of the MAI, and the environment.

A comprehensive stakeholder categorisation, drawn from Freeman's definition [88], the OECD [89], and the IAEA definition [90], is necessary to ensure all stakeholders are correctly identified, along with their influence on the MAI.

We first need to understand what is meant by the term 'Stakeholder'.

According to Freeman: The definition of 'stakeholder' is "any group or individual who can affect or is affected by the achievement of an organisation's purpose"

The Organisation for Economic Co-Operation and Development (OECD) /Nuclear Energy Agency (NEA) Forum on Stakeholder Confidence identifies a stakeholder as:

"any actor-institution, group or individual with an interest in or a role to play in the societal decision-making process".

A useful distinction often made, drawing from the IAEA Handbook on Nuclear Law is between '**statutory**' and '**non-statutory**' stakeholders. This distinguishes between those organisations and bodies that are, by law, required to be involved in any planning, development or operational activity (**statutory**), and those that will be impacted, directly or indirectly by it (**non-statutory**).

In cases of non-compliance against a specific requirement, statutory stakeholders can influence the operation of the vessel through legal recourse. Non-statutory stakeholders may pursue damages or seek an injunction (either a mandatory injunction to perform or a prohibitory notice). Although these groups differ in their formal authority, both play a role in shaping the design, operation, and regulatory framework of the MAI.

In this research, stakeholder categorisation will follow a process consistent with the IAEA approach, defined as follows:

- Statutory stakeholders such as:
 - Regulators, such as IMO, HSE, ITU, Flag-States, and Port Authorities
 - Local or national planning authorities
- Non-statutory stakeholders such as:
 - Insurers
 - Ship operators and owners
 - Crewing agencies
 - Unions
 - Classification societies
 - Pilots

- Standards making bodies
- Cyber security experts – due to the digital nature of the MAI
- Utility services providers (e.g., power and water for land-based ROCs)

While Freeman's definition is widely cited, it can imply an equal degree of influence among stakeholders, which does not reflect the hierarchical structure of the maritime industry. For example, while both regulatory authorities and the refuelling bunker barge operators have the capacity to prevent a ship from sailing, either through regulations (compliance) or by not supplying fuel for the voyage (operational dependencies), the regulatory authority requirements can change within a single voyage and the dynamic nature of such changes need to be considered within the LPM when operating the MAI.

Furthermore, the dimensions of stakeholder's power, legitimacy and urgency, concepts central to Mitchell, Agle, and Wood's stakeholder salience model [91], must be considered within the LPM to ensure stakeholder's power to influence, legitimacy of the stakeholder's relationship and their urgency are addressed, noting the dynamic attribute of urgency will moderate the attributes of power and legitimacy [92]. The strategic timing of stakeholder engagement is equally as important as the precise stakeholder identification and categorisation. For example, engagement with the owners/company and shipyard is typically carried out at the start of the project, while interaction with the manufacturers, and pilotage requirements may occur later in the project. Early engagement with the port authorities can be beneficial, particularly for emergency planning, such as determining responses to a fire on a crewless vessel, or scenarios that require the vessel to immediately leave the berth.

To address the dynamic and evolving nature of stakeholder requirements, a phased or iterative stakeholder engagement process is essential. This approach aligns with each stage of the MAI lifecycle, and facilitates the continuous reassessment of stakeholder concerns, roles, and requirements as the project progresses, ensuring the assurance/safety case can be continuously refined and updated to reflect emerging risks and evolving operational conditions. For example, port diversions, the upgrade of technologies that support the MAI, a change of crew or introduction of a new ROC can bring new stakeholders and associated risks that must be evaluated and managed to maintain an acceptable level of safety.

As illustrated in Table 5-3, the MAI involves multiple stakeholders in the remote control or autonomous operation of the MAI that span three principal domains – *Land, Maritime and Space*, each exerting unique influences on the design and operational framework of the MAI. For example, a land-based ROC located in the UK, would be governed by national regulations such as the UK Health and Safety Executive [93], which may conflict with the maritime requirements set by the maritime regulators. Similarly, satellite communication systems (the space domain) have a direct influence on the assurance/safety case particularly in scenarios, where the terrestrial communication infrastructure is unavailable or unreliable.

Transitioning between autonomous and remotely controlled operational modes further complicates stakeholder interactions and legal obligations. For example, once operations are conducted from a land-based ROC, the legal framework governing land-based laws will become applicable adding new layers of responsibility. Demonstrating continuous compliance with the agreed assurance/safety case across all operational conditions is essential because the dynamic nature of the MAI, such as changes in operational conditions (manual, remotely controlled, autonomous), regulatory jurisdictions or voyage conditions, can introduce new or previously unconsidered risks. Consider a vessel initially approved to operate between two fixed ports, is diverted to an alternative location not previously considered within the LPM. This may introduce new risks that render the prior assurance/safety case incomplete with no guarantee that the risks will remain tolerable. Such changes require prompt and transparent engagement with all relevant stakeholders to ensure they understand the operational implications, can fulfil their respective responsibilities, and are able to respond effectively to any emerging risks.

To address the complexity and inherent risks associated with simultaneous multi-modal operations, rigorous risk assessments must be conducted as outlined in Section 5.2.7. These assessments should explicitly consider the specific roles, responsibilities, and information flows among all relevant stakeholders to ensure the operational risks remain tolerable under all defined operational conditions. For example, port authorities may need to collaborate with technology providers to manage dynamic information exchanges, to ensure the operational risks remain tolerable under defined port/vessel conditions. This multi-modal and cross-domain approach highlights the need for an adaptive and function-specific operational model that aligns with business objectives, while meeting agreed regulatory and safety requirements.

Ultimately, failing to include key stakeholders, misinterpreting their roles, incorrectly categorising them, or neglecting engagement at critical project junctures can significantly compromise the MAI's ability to meet safety objectives and secure the necessary regulatory certifications. Therefore, a flexible and iterative stakeholder management strategy is essential, one that continuously aligns with the safety, operational, technological, and regulatory landscapes throughout the lifecycle of the MAI.

As shown in Table 5-3 the number of stakeholders decreases from '*Forty One*' in remotely controlled operation to '*Twenty Two*' in autonomous operation. A larger stakeholder count increases the number of points of interface, introduces the potential for greater requirement variability and expands the evidence workload in developing and maintaining the assurance/safety case. In contrast, a smaller number of stakeholders does not relax or imply simplification of the assurance problem, as responsibilities previously exercised by ROC personnel and associated service providers are reallocated to the autonomous functions and system design authorities, thereby increasing the criticality of the remaining stakeholders/actors, and interfaces. Accordingly, assurance emphasis shifts from human-centred operational controls (e.g., handover protocols) to design-time controls, such as, explicit LoP's that do not rely on remote intervention, pre-defined and verified fallback states, and rigorous configuration and change governance, such that the safety/assurance case continues to support the claim of 'Acceptably Safe'.

Actors/Stakeholder	Environment	Statutory Stakeholder	Non Statutory Stakeholder	Remote Control of the MAI	Autonomous Operation of the MAI
Bunker/refuelling companies	Maritime		X	X	X
Classification Societies	Maritime		X	1	1
Connectivity Providers	Land	X		X	
	Space	X		X	
Crewing agencies	Maritime		X	X	
Cyber security providers	Land		X	X	
Designers	Land		X	X	
	Maritime		X	X	X
Dock Workers	Maritime		X	X	X
Emergency services	Maritime	X		X	X
	Land Police	X		X	
	Land Fire	X		X	
	Medical		X	X	
Flag State	Maritime	X		X	X
Insurers	Land		X	X	
	Maritime		X	X	X
ISA	Maritime		X	X	X
	Land		X	X	
Manufacturers	Maritime		X	X	X
	Land		X	X	X
	Space		X	X	
Owner/Company	Marine		X	X	X
	Land		X	X	
	Space		X	X	
Pilots	Maritime		X	X	X
Planning authorities	Land	X		X	
Port Authorities		X		X	X
Port state control	Maritime			X	X
Repairers	Land		X	X	
	Maritime		X	X	X
Regulatory Authorities	Land	X		X	
Salvors	Maritime		X	X	X
Security organisations	land		X	X	
Shipyard	Maritime		X	X	X
Standards making bodies	Land		X	X	
	Maritime		X	X	X
Trade Unions	Land		X	X	
	Maritime		X	X	
Tug companies	Maritime		X	X	X
Utility companies, e.g. Electricity/Water	Land		X	X	
Vetting agencies	Maritime		X	X	X
	Land		X	X	
VTS	Maritime		X	X	X
Waste disposal companies	Maritime		X	X	X
	Land		X	X	X
Total number of stakeholders		9	34	41	22

Table 5-3: Comparison of stakeholders involved in remote control or autonomous operation of the MAI

Note: engaging a Classification Society may not be mandatory for the project; however, if one is selected, their requirements must be met in accordance with contractual obligations.

5.2.5 Voyage Conditions.

The term 'voyage conditions' refers to the specific factors that must be considered throughout the MAI lifecycle. These conditions are critical for evaluating risks and ensuring they remain tolerable. Consideration should be given to conditions that impact safety, lead to intolerable risks, or hinder the ability to complete the voyage plan.

The three 'voyage conditions' defined in this research are:

- Normal condition - the absence of a reasonably foreseeable abnormal or emergency condition, while operating the MAI within its design intent.
- Reasonably foreseeable abnormal event [94] - an event, incident or failure that has happened and could happen again or is planned for. These conditions may degrade performance but should not result in an intolerable risk, Examples include:
 - a total loss of the main source of electrical power, due to an overcurrent trip (Source: LR Rules Pt 6, Ch 1, 1.6.8.).
 - activation of an automatic power limitation due to a gas turbine high-power turbine inlet temperature. This can result in a reduction of available power to the vessel and a reduction in propulsion capability (Source: LR Naval Rules Vol 2, Pt2, Ch2, Section 10.).
 - operating in areas where adverse weather conditions are reasonably predictable and statistically significant, such as operating in the North Atlantic in winter, where research carried out for revised and adopted new wave data for the North Atlantic as defined in the IMO MSC 108/19 [95], should inform the risk assessment if the vessel is operating in that area.

- **Emergency condition** – a non-routine situation or event that necessitates prompt/immediate action to mitigate hazards or adverse consequences to human life or to the environment (Source: derived from IAEA safety glossary 2018) [95]. Examples include:
 - Collision avoidance – a requirement to alter the vessel's speed or direction to avoid a collision. If there is a degradation of the function, the ability to execute this manoeuvre may be compromised. On a crewed ship, the STCW-trained crew could intervene to mitigate the risk by manually controlling the steering gear or overriding an automatic slowdown or shutdown function.
 - Environmental damage¹³ – numerous maritime accidents have resulted in significant environmental damage, such as the Atlantic Express, Amoco Cadiz, and the Torrey Canyon. In March 2021, the container ship Ever Given¹⁴ was struck by strong winds and ended up wedged across the waterway effectively closing it for six days. The accident report states that *“the VTMS¹⁵, pilots and master had not properly evaluated bad weather conditions, especially strong winds and reduced visibility, as a risk condition for a VLCC¹⁶ vessel with large area exposed to the wind”*.

The risk analysis detailed in Section 5.2.7 will need to consider events, incidents or failures under all three conditions to ensure the risks remain tolerable to the satisfaction of the relevant stakeholders. Whilst the distinction between reasonably foreseeable abnormal and emergency conditions might be somewhat judgemental, consideration of the concept and voyage plan can help to discriminate between them. Note that the introduction of an MAI might alter the categorisation of these conditions where for example, an abnormal condition that can be ‘managed’ by personnel on board might escalate to an emergency on an uncrewed autonomous vessel.

¹³ <https://shipwrecklog.com/log/history/atlantic-empress/> - accessed 28th April 2025

¹⁴ <https://gcaptain.com/wp-content/uploads/2023/07/Final-Investigation-Report-Ever-Given-23-March-2021.pdf> - accessed 28th April 2025

¹⁵ VTMS – Vessel Traffic Management Services

¹⁶ VLCC – Very Large Crude Carrier

5.2.6 Operational Conditions.

Operational conditions define the methods by which control over the vessel's functions is exercised. These conditions, adapted from ISO TS 23860:2022 [97], describe the Operational Conditions of the MAI as follows:

- **Manual** – ship systems, processes, or equipment are directly controlled by the crew on board. The vessel operates under the command of a Master, as specified by UNCLOS Article 94.4b.
- **Remote** – control or monitoring of ship functions is performed by an individual who may be on or off the vessel.
- **Autonomous** – one or more of a ship systems, processes, or functions, under certain conditions, are designed and verified to be controlled by *automation*, without human intervention.

During a single voyage, it may be necessary to changes the operational conditions in response to technical, regulatory, or company requirements, examples of which are:

- **Technical Requirements:** a system malfunction, degradation of a function, or operational safety requirement may necessitate switching between the operational conditions. For example: isolating autonomous functions when personnel are on board.
- **Regulatory Requirements:** Port Authorities may prohibit autonomous operation of the vessel when entering or exiting the port.
- **Company Requirements:** Company protocols may mandate specific operational modes, such as requiring remote control during berthing operations instead of manual or autonomous modes.

Where operational conditions change, it is essential to consider the safety, security, legal, and stakeholder requirements. In cases where the vessel functions alternate between autonomous or remote control, the risk analysis should confirm that risks remain tolerable. This scenario represents a unique use case that must be addressed during the concept phase of the LPM.

5.2.7 Hazard and Risk Analysis.

The objective of the hazard and risk analysis within the LPM framework is to systematically identify and evaluate all reasonably foreseeable hazards associated with the MAI. The methods and tools employed for hazard identification should be proportionate to the potential risks posed by the MAI, the nature of the operational risks, whilst also considering the complexity of the project.

To ensure comprehensive and effective hazard identification and risk analysis, it is essential to involve suitably qualified and experienced professionals representing all relevant domains, including maritime operations, land-based control and connectivity, space-based communication systems, and the legal sector. This multidisciplinary expertise is critical to capturing the complete range of risks inherent to the MAI, particularly given its SoS structure.

This research proposes that the methodologies for hazard and risk identification and analysis should be explicitly defined, justified, and agreed upon by relevant stakeholders. Such agreement is vital to establishing a compelling body of evidence for acceptance by the regulatory authorities.

However, the inclusion of diverse expertise while providing a rich pool of knowledge and skills also introduces challenges such as aligning differing professional perspectives, reconciling domain-specific terminologies, and ensuring consistency in the documentation and interpretation of hazards. Addressing these challenges will be fundamental to achieving a coherent, integrated, and robust risk management process for the MAI as illustrated in the following examples:

5.2.7.1 Differences in industry practices and standards.

Each industry involved in the MAI brings its own established standards, regulatory frameworks, operational practices, and methodologies for hazard and risk management. These divergent practices can lead to inconsistencies in terminology, risk thresholds, and accountability structures, making it essential to develop a standard operational framework that supports both operability, and regulatory compliance. For example:

- Maritime industries focus on regulations set by the IMO and where required the rules of the Classification Society.

- Land-based operations might adhere to standards such as ISO 45001 for occupational health and safety. [98]
- Communication providers will follow requirements defined by the ITU

Harmonising these varied approaches requires identification of commonalities and differences, aligning objectives, and fostering mutual understanding among stakeholders. Where differences occur, these need to be agreed based on technical, safety, and legal grounds. For example, a fire alarm in the ROC will probably require evacuation of the space (as required by company procedures) with re-entry only possible after authorisation has been given by the emergency services. On a crewed vessel, the treatment of a fire alarm does not normally require external assistance, and the crew do not evacuate the vessel until ordered to do so by the ship's master.

5.2.7.2 Terminology differences.

The diverse backgrounds of the stakeholders involved in the MAI can lead to variations in the interpretation of key terms and concepts. For example, terms such as 'watchkeeping', 'handover' and 'tolerability of risk' might have different meanings depending on the industry. Misalignment in the understanding of terminology can lead to confusion, miscommunication, and inconsistent application of risk analysis and assurance/safety processes. To mitigate this threat, it is essential to establish a common vocabulary or glossary that is agreed upon by all relevant stakeholders to ensure clarity and consistency throughout all phases of the MAI's - LPM.

As an example, the term 'System' is interpreted differently across domains. In the maritime sector ISO/IEC 15288 defines a system as – *'system a combination of interacting elements organised to achieve one or more stated purposes'*.

By contrast ISO 45001 provides a context-specific definition for a management system within Occupational Health and Safety (OHS)] – *'set of interrelated or interacting elements of an organisation to establish policies and objectives and processes to achieve those objectives'*.

While ISO/IEC 15288's [30] definition applies to systems of any domain, ISO 45001's [98] definition is narrower in scope, focussing on the management structure and process needed to meet OHS objectives. For the MAI, it is necessary to select or adapt definitions that maintain clarity across domains while ensuring they are appropriate for the specific operational and regulatory context.

The legal domain offers further variation. Merryman states that the legal system is: *'an operating set of legal institutions, procedures and rules'* [99], while Blacks Law dictionary defines a system as: *'detailed procedures, methods and routines to carry out an activity, problem solve or perform a duty'*, and as a *'purposeful organised structure that is regarded as a whole and consists of interdependent and interrelated elements'* [100].

These definitional differences are not semantic; they shape how system boundaries, responsibilities, and interactions are understood within the MAI. Clear alignment on a suitable definition within the LPM is essential to avoid ambiguity, ensure cross-domain coherence, and maintain operational consistency.

5.2.7.3 Conflict in priorities and objectives.

Stakeholders from different sectors may prioritise risks differently based on their specific operational focus. For example:

- Legal experts may prioritise regulatory compliance and liability mitigation.
- Engineers might focus on technical safety and assurance.
- Environmental specialists could emphasise minimising ecological impact.
- Land-based organisations may emphasise HSE requirements over the safety of the vessel.

Developing a balanced risk management framework that addresses these competing priorities equitably is essential for maintaining alignment and ensure the evidence presented to the regulatory authorities allows them to issue the required approvals/acceptance for the MAI.

5.2.7.4 Variability in experience with autonomous systems.

The relative novelty of autonomous systems within certain sectors results in differing levels of familiarity and expertise. Some industries, such as the space sector, have extensive experience with remote or autonomous operations, whereas others, such as the traditional maritime sectors, are comparatively less familiar. In addition, certain industries, such as the communication sector, may not fully appreciate the extent to which their systems could influence the safety of the MAI under certain operational conditions.

This disparity in experience and awareness can create gaps in understanding, necessitating targeted stakeholder engagement, to ensure all relevant parties can effectively contribute to the hazard and risk analysis process.

5.2.7.5 Coordination across geographies and jurisdictions.

Where the MAI's operation spans multiple regions, each with its own regulatory requirements, coordinating the perspectives of international stakeholders becomes increasingly complex. Differences in legal requirements, enforcement mechanisms and cultural attitudes toward risk, may lead to conflicting requirements. To address this, establishing clear lines of communication and decision-making protocols can help mitigate these challenges.

5.2.7.6 Ensuring consistency in outputs.

The diverse expertise of the team can result in varied approaches to risk assessment, potentially leading to inconsistent outputs. To address this, a standardised framework for the hazard and risk analysis process is essential. This framework should include clear guidelines on methodology, deliverables, and reporting formats, ensuring that outputs are comprehensive and comparable across disciplines.

5.2.7.7 Summary

In summary, these multidisciplinary challenges underscore the complexity inherent in the hazard and risk analysis for the MAI. They highlight the necessity of a cohesive, standardised, and transparent approach to risk management that bridges the gaps between diverse industry practices, regulatory expectations, and stakeholder perspectives. By recognising and addressing these challenges through shared terminology, harmonised frameworks, and collaborative engagement, it becomes possible to develop a robust and credible assurance case that supports the claim of ‘Acceptably Safe’ operation within a dynamic, multi-domain environment. Ultimately, this integrated approach is essential not only for regulatory compliance and certification but also to fostering stakeholder confidence and ensuring the long-term operational integrity of the MAI.

5.2.8 Overall Safety Requirement.

A unique contribution of this thesis is the development of a ‘Safety Process Model’ (SPM) for the MAI, as illustrated in Figure 5-4. The primary function of the SPM within the context of the MAI is to provide a structured methodology for deriving the safety requirements, determining whether a claim of ‘Acceptably Safe’ has been substantiated, verifying that stakeholder requirements have been fulfilled, and supporting the creation and evaluation of the compelling body of evidence for regulatory submission and review.

The ‘SPM’ has several core elements each addressing a distinct aspect of the assurance/safety requirements for the MAI. Collectively, these components form a systematic framework for identifying, evaluating and verifying the outcome of each stage of the LPM, with emphasis on independent verification, prior to regulatory submission.

Within the SPM, the directional relationships between elements are expressed as either ‘informs’ or ‘influence’. This distinction is deliberate:

- ‘informs’ represents the transfer of information, data, or evidence from one element to another, where the receiving element may use the input to support decisions but is not necessarily required to alter its approach or scope.
- ‘Influences’, by contrast, indicates a prescriptive relationship in which the upstream element actively shapes, constrains, or modifies the requirements, methods, or outcomes of the

downstream element. Changes in an influencing element require corresponding changes downstream.

In certain cases, an element may both ‘influence and inform’ another, meaning it provides factual input while also imposing requirements that directly affect how the downstream process is executed, for example: the output of the Independent Verification has influence and informs the Safety Assessment process. This distinction ensures that the SPM captures both the logical flow of safety evidence and the dependency relationships that govern assurance and approval of the MAI, thereby establishing a traceable and defensible framework through which compliance can be demonstrated.

To enhance credibility and confidence in the documented safety report, the SPM requires an Independent Safety Assessment to be carried out, aligning with the principles defined in the nuclear sector [101], and the UK Defence Security Authority [102]. This assessment ensures that the safety aspects of the MAI have been subjected to rigorous and continual oversight by a third party with no financial interest or connection to the project and serves to identify potential biases or omissions in the safety assessment process, whilst ensuring the overall Goal, as defined in the LPM has been effectively achieved. This is further expanded in Section 5.2.1.

This approach represents a fundamental change from conventional crewed vessel acceptance processes, which typically rely on acceptance from a recognised Classification Society based on compliance with predefined and established rules. Given that the MAI consists of elements that extend beyond the scope of the traditional maritime domain, the requirement for independent verification is a critical enhancement in the assurance process for the MAI.

An additional requirement in the SPM is the emphasis on an iterative approach in the development of the compelling body of evidence, requiring greater collaboration among stakeholders. This approach could require revisions to existing contractual frameworks, particularly given the complexity and cross-disciplinary nature of the MAI. As noted in [103]; *‘The marine sector, with its fragmented approach to system integration, will need to adopt a process that is not solely controlled by commercial and contractual agreements’*. While this issue lies outside the direct scope of this thesis, it remains a relevant consideration within the broader context of the MAI.

The 'Safety Assessment' element embedded within the SPM links stakeholder requirements to the 'Safety Approach', informs the selection of the 'Safety Analysis' methodology, and influences the 'Operational Considerations' for the MAI. While the SPM does not specify methodologies, tools, or techniques for the safety analysis, it requires that these methods be explicitly defined, justified, and agreed upon by the relevant stakeholders. The methodologies must consider the complexity of the MAI and whether established techniques provide sufficient evidence that the MAI is 'Acceptably Safe' to operate in a defined context of use. If traditional methods are deemed inadequate, as stated by Leveson, advanced techniques such as Safety Assurance of autonomous systems in Complex Environments (SACE) and System -Theoretic Process Analysis (STPA) [104] [105] may need to be considered.

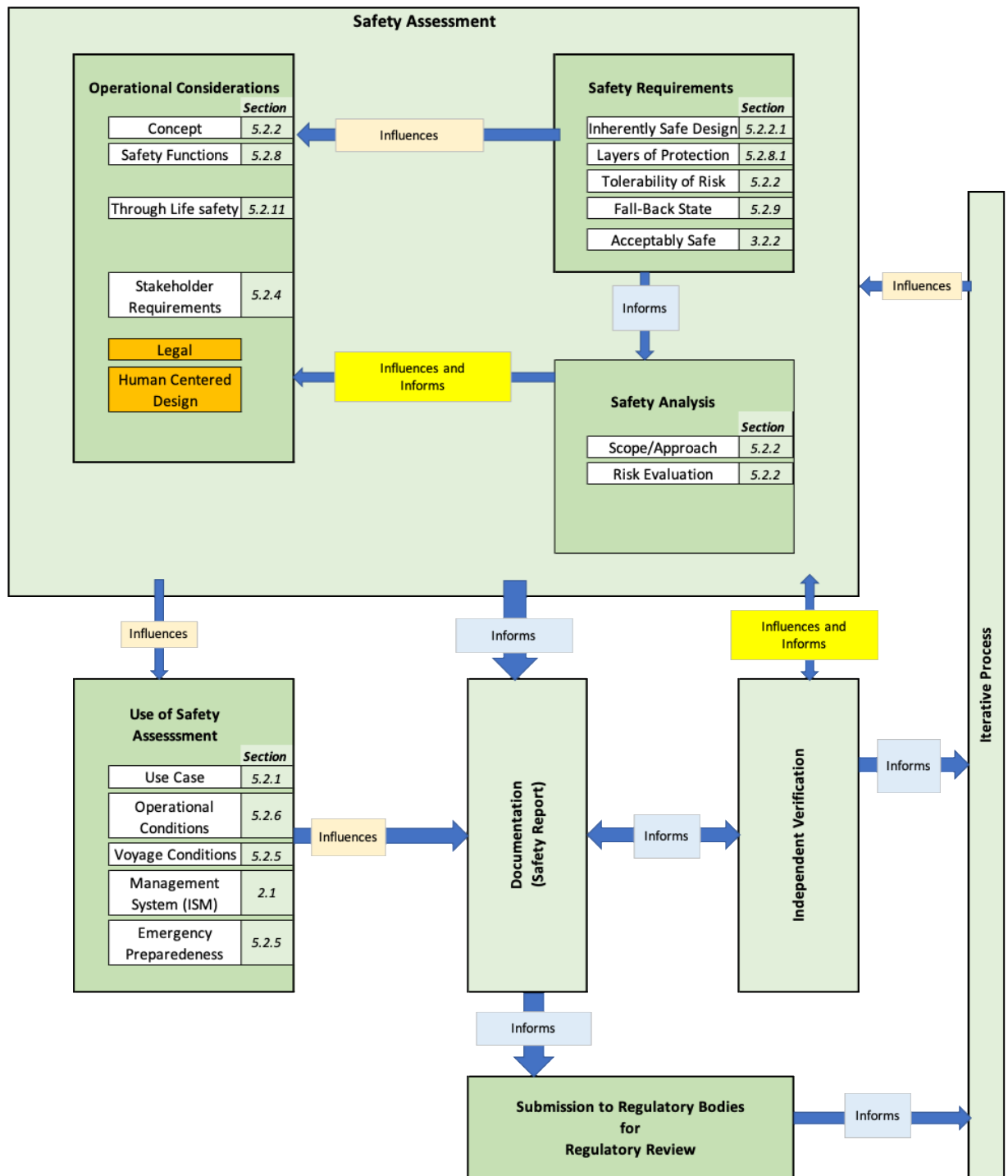


Figure 5-4: Safety Process Model (SPM) for the MAI.

The operational considerations will be defined by the company and the relevant stakeholders. Safety functions will need to be agreed upon to ensure the risks do not become intolerable throughout the MAI lifecycle. The output from the 'Safety Assessment' influences the way in which the MAI can be used, whether the voyage conditions can be achieved and how the International Safety Management Code (ISM) [127]¹⁷ needs to consider the operation of the MAI at a SoS Level.

As illustrated in Figure 5-4, the outputs of the interrelated SPM elements ultimately converge in the Safety Report. This document is the tangible outcome of the Safety Assessment, integrating the information and constraints conveyed through both 'informs' and 'influences' relationships within the model. The Safety Report provides the documentary evidence necessary to substantiate safety claims and to ensure that the risks associated with the MAI do not become intolerable. It must be sufficiently comprehensive and detailed to support the conclusions reached in the Safety Assessment while also providing a robust foundation for independent verification and regulatory review.

To facilitate effective regulatory engagement, the report format should be standardised, clear, and accessible to all relevant stakeholders. As discussed in Section 4.1.7, failure to consider stakeholders' comprehension can result in assumptions that cannot be validated, potentially escalating into intolerable risks.

Finally, as shown in Figure 5-1 (LPM), the SPM (Figure 5-4) provides the structured means by which the safety requirements are derived, assesses, verified and consolidated into the compelling body of evidence needed to support the claim of 'Acceptably Safe'. The SPM links the LPM stages across the MAI lifecycle, ensuring traceability from Goals to the Safety Report. Consistent with Figure 5-1 (LPM) the SPM identifies 'Legal' and 'Human-Centred Design' as critical and influencing elements under all operational and voyage considerations. These aspects, while outside the primary scope of this research, are identified as key areas for future work, to ensure stakeholder requirements are fully addressed, to formalise the allocation of legal responsibility and accountability across all relevant stakeholders [65], and to define capabilities under all operational and voyage conditions, supported by a configuration-controlled allocation model.

¹⁷ IMO-ISM adopted in 1993 by resolution A.741(18). The ISM Code is to provide an international standard for the safe management and operation of ships and for pollution prevention.

5.2.8.1 Layers of Protection.

The purpose of introducing the principles of 'Layers of Protection (LoP)', is as stated by the Office for Nuclear Regulators [106]:

***'to provide a series of independent barriers aimed at preventing faults in the first instance and ensuring appropriate protection and mitigation of accidents in the event that protection fails.'* ONR.**

In the context of crewless vessels, the removal of STCW-trained crew removes a critical human intervention layer of protection. This shift necessitates a comprehensive reassessment of risk management strategies within the MAI, to ensure that failures do not result in an uncontrolled or rapid escalation to an emergency condition. A unique contribution to this thesis is the development of the Layers of Protection framework specifically designed for application within the MAI.

Although the IMO does not explicitly require LoP's to be defined within the statutory instruments, the concept of layered risk mitigation is evident in a range of existing regulatory requirements. For example, the treatment of fire is addressed within various chapters of SOLAS, including:

- **SOLAS ChII-2 Construction** – Fire protection, fire detection and fire extinction. This requires structural fire boundaries and passive protection systems such as fire doors.
- **SOLAS ChII-1 Part D** - Electrical installations – mandates an emergency source of electrical power to supply the fire detection and fire alarm system for the period specified, ensuring operational resilience in the event of a loss of the main source of electrical power.
- **STCW Convention Chapter V1/3** - Outlines mandatory minimum requirements for training in advanced firefighting, equipping crew with the skills to prevent, control and fight fires on board.
- **SOLAS ChIII – Lifesaving appliances and arrangements** - Includes requirements for Emergency Training and drills - Regulation 19.

The development of the 'Layers of Protection' model was assessed against the 'Bow Tie' methodology for risk assessment in the context of the MAI. The Bow-tie methodology is superior when the aim is rapid, shared understanding around specific top events, especially across mixed technical and non-technical stakeholders. It visualises threats, barriers, and consequences in a way that supports early

hazard elicitation, regulatory and insurer engagement, organisational controls, and post-incident learning.

In a prescriptive and regulated setting, bow-ties can provide sufficient assurance evidence for regulatory acceptance. However, in the context of the MAI, the method was evaluated and found unsuitable as a primary assurance artefact because the MAI's requirement to consider changing operational conditions (manual/remote/autonomous), changing voyage conditions (normal/RFAE/emergency), authority transfers (ROC \leftrightarrow ROC/ROC \leftrightarrow onboard), and jurisdictional changes within a single voyage, renders a bow-tie as a context fixed representation that would need to be redrawn and re-validated for each context of use. Accordingly, this thesis develops a LoP framework that integrates with the LPM, SPM and MAI-DE, so that independence, performance criteria, and per-voyage validity can be specified, verified, and governed within the assurance/safety case.

However, there is currently a gap in the explicit definition and structured application of LoP principles within the unique context of the MAI, particularly in addressing the removal of STCW-trained crew as a direct intervention layer of protection. To address this gap this thesis develops five distinct layers of protection for the MAI, intentionally designed to be as independent as possible to maximise their effectiveness and provides a structured, scalable and stakeholder adaptable framework for implementing LoP within the MAI. It acknowledges that the number and scope of layers will be refined by the relevant stakeholders based on specific operational and regulatory requirements.

While the principle of LoP is well-established in safety critical industries, its explicit definition and structured integration within the MAI represents a unique contribution. The removal of STCW-trained crew eliminates a key human layer of defence, increasing reliance on system design to prevent, contain, and respond to faults. Within this context, the development of the LoP framework is not merely a theoretical exercise but a practical necessity for maintaining control and avoiding hazards escalating towards an emergency condition.

This structured integration of layered protection into the MAI lifecycle not only addresses existing regulatory gaps but also establishes a foundation upon which future autonomous or remotely

controlled operations can be assessed to ensure appropriate risk mitigation strategies are acceptable to the relevant stakeholders. It ensures that risk mitigation strategies are aligned with stakeholder expectations and acceptable within a dynamic operational context.

The following section builds upon this foundation by introducing the MAI Design Envelope (MAI-DE), which formalises the integration of Concept, Voyage Conditions, and Layers of Protection into a unified framework that supports design, assurance, and regulatory engagement throughout the LPM.

Layers of Protection				LPM Step	
Level	Objective	Defence/Barrier	Guidance	Concept	Voyage Condition
Level 1	Prevention of abnormal operation and failures by design	Conservative design, high quality in construction, maintenance and operation in accordance with appropriate safety criteria, engineering practices and defined quality standards	Compliance with specified standards	Inherently Safe Design	Normal
Level 2	Prevention and control of abnormal operation and detection of failures	Control, limiting and protection systems, other surveillance features and operating procedures to prevent and minimise damage from failure.	Compliance with specific standards and outcome from the risk analysis of the system under consideration	Fault Tolerant	RFAE
Level 3	Control of faults within the design basis to protect against escalation to an accident	Engineering safety features, multiple barriers and accident or fault control procedures	Compliance with specific standards and outcome from the risk analysis and requirements from the shipowner/company	Fault Tolerant	RFAE
Level 4	Control of severe ship or infrastructure conditions, in which the design basis may be exceeded, including protecting against further fault escalation and mitigation of the consequences of severe accidents	Additional measures and procedures to protect against or mitigate fault progression and for accident management	Severe ship or infrastructure conditions could include fire, flooding, or evacuation of a ROC due to environmental conditions, landslide, earthquake, terrorist attack etc.	Fault Tolerant/Emergency	RFAE/Emergency (Tolerable)
Level 5	Mitigation of accident consequences through emergency responses	Emergency control and on-off site emergency response (e.g. salvage vessels, fire-fighting tugs, land based emergency services, etc)	An emergency condition will be declared by the owner/operator. Example: Vessel out of operation (not under command) and drifting towards an object, evacuation of a ROC with no possibility of transfer of control to another ROC/remote operator, etc.	Emergency Condition	Emergency (Intolerable)

Table 5-4: Layer of Protection Model for the MAI (LoP)

5.2.8.2 The MAI Design Envelope.

This section presents one of the unique contributions of this research through the development of the Maritime Autonomous Infrastructure Design Envelope (MAI-DE) which builds upon the Layers of Protection principles within the LPM and integrates them with the concept definition and voyage conditions. As illustrated in figure 5-5, the MAI-DE provides the relevant stakeholders with a structured and repeatable method to determine whether the layers of protection and the design basis of the safety systems are sufficient to support a claim of 'Acceptably Safe' under defined operational conditions.

While traditional safety frameworks have proven effective for conventional crewed operations, their direct application present limitations when applied to the autonomous and remote operation of the MAI. In particular, the absence of human intervention as a layer of protection, necessitates a re-evaluation of how the LoP principles are specified, validated, and assured within the MAI context.

Starting with the optimal conditions for the MAI, which is: Inherently Safe Design – Normal Operation - Level 1 (LoP) which is designed to eliminate the hazards and prevent abnormal conditions occurring.

Level 1 event – Prevention of deviations from normal operations.

Inherently Safe Design	Normal Operation	Level 1
Elimination of the hazards	The absence of a reasonably foreseeable or emergency condition and the MAI is operated within the design intent.	Prevention of abnormal operation and failures by design

Level 2 – Detecting and controlling deviations, and **Level 3** – Activation of engineering features, provide technical and procedural barriers to prevent the event escalating towards an emergency condition. Examples include the use of protection systems to allow control under a, degraded but safe mode of operation.

Level 4 - corresponds to an emergency event where the risks remain tolerable and are managed through engineered design features, automated response functions, or the direct intervention of qualified and trained personnel. An example would be the abandonment of a vessel, wherein the trained on-board crew are able to execute pre-defined procedures, such as mustering at survival craft stations as required by the IMO- STCW Code. The act of abandoning the ship can be considered as a tolerable risk, largely attributable to the preparedness and training of the crew, even though the underlying cause of the abandonment of the ship may constitute a level 5 event.

For a land-based ROC, a parallel example would involve the evacuation of personnel due to an uncontrollable situation, such as fire, flood or earthquake. In such cases, although the initiating event may have escalated beyond the capacity of the standard protection measures, the existence of robust evacuation procedures, combined with trained personnel, enables the risk to remain tolerable until external emergency services intervene.

Level 4 event – Limiting consequences and preventing escalation.

Emergency	Tolerable Risk	Level 4
'Emergency': an event or situation which threatens serious damage to human welfare or threatens serious damage to the environment.	At this level, the risks remain tolerable and managed through automated systems and human intervention by qualified and trained staff to prevent further escalation.	The fourth layer is designed to limits the consequences of an event and prevent escalation from failure of the third level of defence.

Ultimately, level 5 reflects conditions where all internal layers of protection have been exhausted or rendered ineffective, necessitating external assistance to be provided to contain the event.

Level 5 event – Emergency response and external intervention.

Emergency	Intolerable Risk	Level 5
'Emergency': an event or situation which threatens serious damage to human welfare or threatens serious damage to the environment.	In this level the risks become intolerable and may require external assistance as all other levels have failed to prevent escalation of the event.	Responding to the consequences of an event that cannot be contained within the preceding layer.

By mapping these LoP levels against defined voyage conditions, the MAI-DE provides a comprehensive operational safety boundary. It enables stakeholders to identify not only the acceptable performance envelope of the MAI but also the thresholds at which operational, regulatory, or emergency interventions must occur.

The value of the MAI-DE lies in its context-specific applicability, it can be applied to any MAI configuration and operational profile, allowing for variations in risk tolerability, stakeholder requirements, and regulatory constraints. While the MAI DE provides a comprehensive framework for integrating inherent safety, fault tolerance, and emergency response, its effectiveness in addressing the unique challenges presented by the MAI is demonstrated through the use cases presented in 5.2.8.3 below.

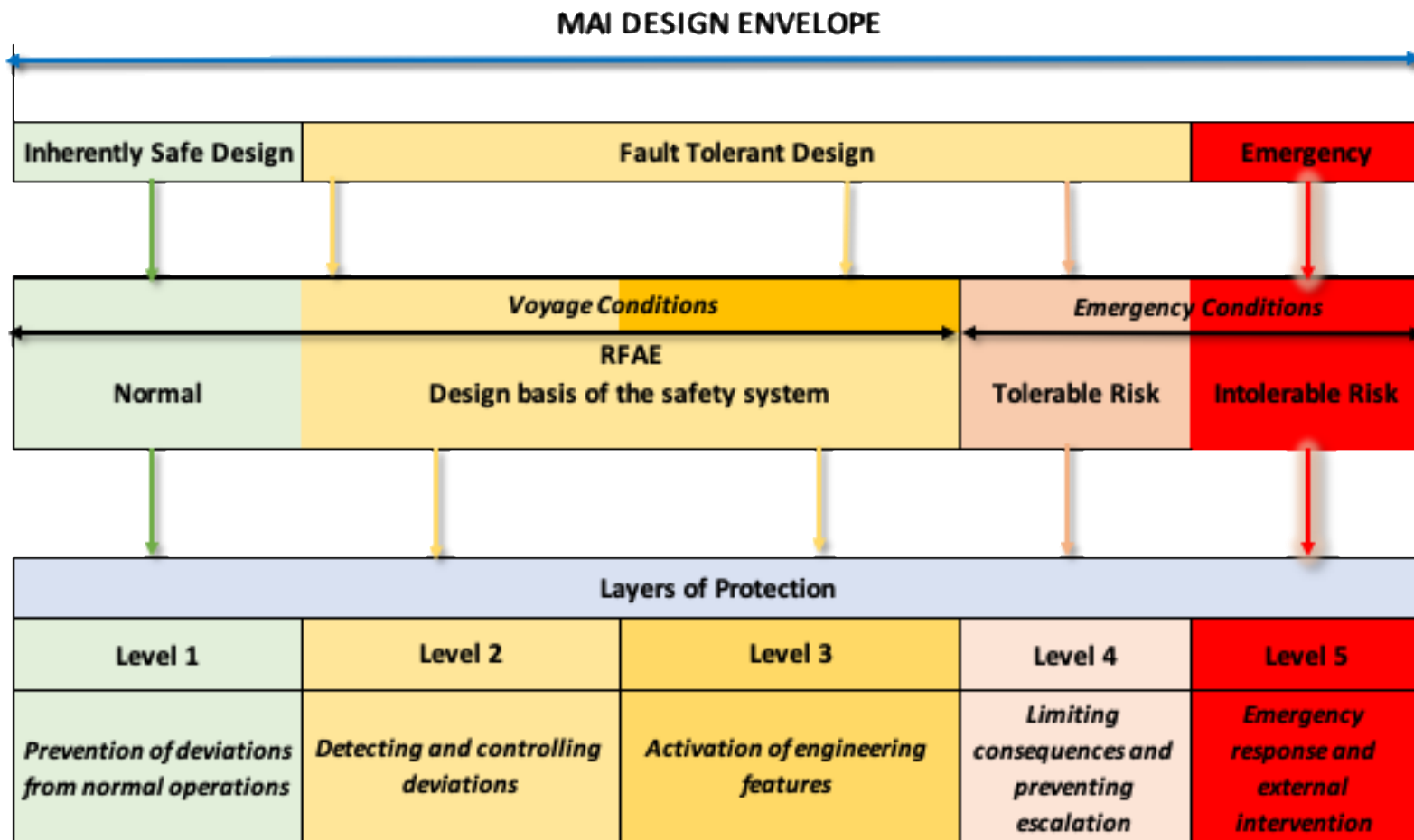


Figure 5-5: MAI Design Envelope

5.2.8.3 Examples in the application of the MAI Design Envelope.

To illustrate the practical implementation of the layers of protection (LoP), and the MAI-DE under dynamic voyage conditions, this section presents three representative scenarios. Each scenario demonstrates how the LoP, the voyage conditions and the MAI-DE interact to manage risks and support the assurance/safety process under different operational conditions

- Case 1 – a fire incident escalating from normal to an emergency condition;
- Case 2 – a navigational hazard management scenario;
- Case 3 – a failure involving the loss of electrical power;

Level 1- Prevention of deviations from normal operations:

The primary layer aims to prevent deviations from normal operations by applying inherently safe design principles. This involves deriving clear requirements, identifying, and aligning on applicable standards, and implementing systematic processes and procedures across the lifecycle of design, manufacturing, construction, maintenance and operation of the MAI. These measures are intended to ensure that risks remain within tolerable limits.

Case 1.	<i>fire prevention through design is preferable to fire detection and extinction.</i>
Case 2.	<i>normal operation provides clear navigational passage with no restrictions from berth to berth.</i>
Case 3.	<i>no single point event should result in the complete loss of electrical power.</i>

Table 5-5: Level 1 Scenarios

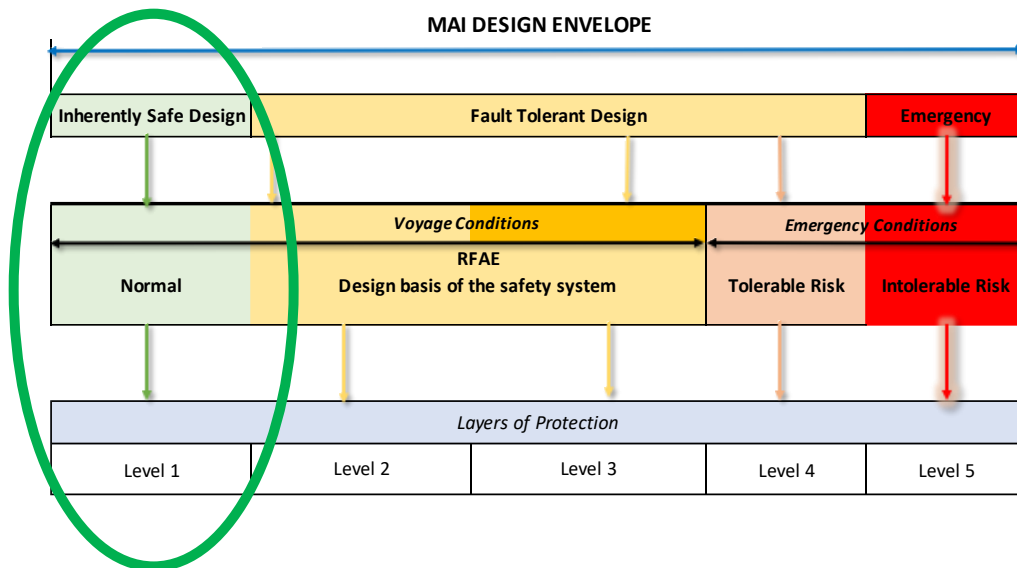


Figure 5-6: Level 1- Prevention of deviations from normal operations

Level 2 - Detecting and controlling deviations.

The second layer focusses on detecting and controlling deviations from the normal operational parameters. This necessitates the integration of control, limiting and protection systems that demonstrate compliance with the relevant standards and specific requirements emanating from LPM stages. Where a reasonably foreseeable abnormal event takes place, these measures are designed to either prevent further escalation or mitigate the consequences of the event. This aligns with the principle of fault tolerance, with mitigations being relatively simple and easily understood.

Case 1	<i>fire detection system is a system designed to detect a reasonably foreseeable abnormal event (a fire) to alert the relevant stakeholders, enabling a timely response.</i>
Case 2	<i>requirement to hold position is a deviation from a normal operational parameter. This will require a means of demonstrating compliance with the requirement, e.g. anchoring or its equivalent.</i>
Case 3	<i>total loss of electrical power is a RFAE. The protection and control systems should be designed to ensure that a total loss of electrical power is avoided as far as practicable. To control the risk the MAI could, through design, ensure that a total loss of electrical power is extremely unlikely to occur.</i>

Table 5-6: Level 2 Scenarios

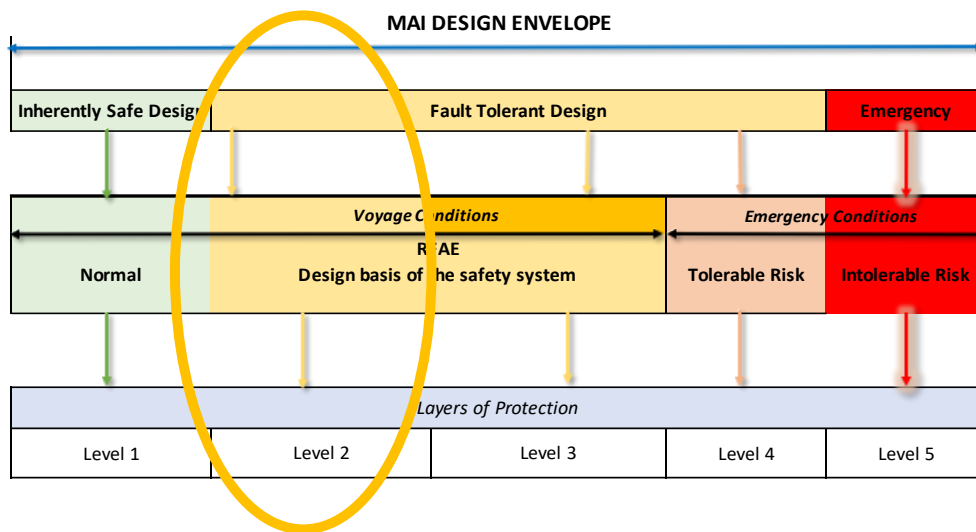


Figure 5-7: Level 2 - Detecting and controlling deviations

Level 3 - Activation of engineered safety features

If an event cannot be managed within the first two layers, the third layer involves the activation of engineered safety features and safety systems, as well as the implementation of processes and procedures. These measures, guided by the owner tolerability of risk requirements, aim to prevent the event escalating towards an intolerable risk.

Case 1	<i>automatic release of a fixed water based local application fire-fighting system (FWBLAFS) that serves to contain and manage the fire risks.</i>
Case 2	<i>If the position holding technology fails or degrades to a point where the risks are escalating towards an intolerable risk. e.g. the vessel could end up drifting. The system will likely fall through this level very quickly and move into level 4.</i>
Case 3	<i>activation of protection systems (e.g. power management and disconnection of non-essential services) to prevent the electrical trip from occurring in the first place.</i>

Table 5-7: Level 3 Scenarios

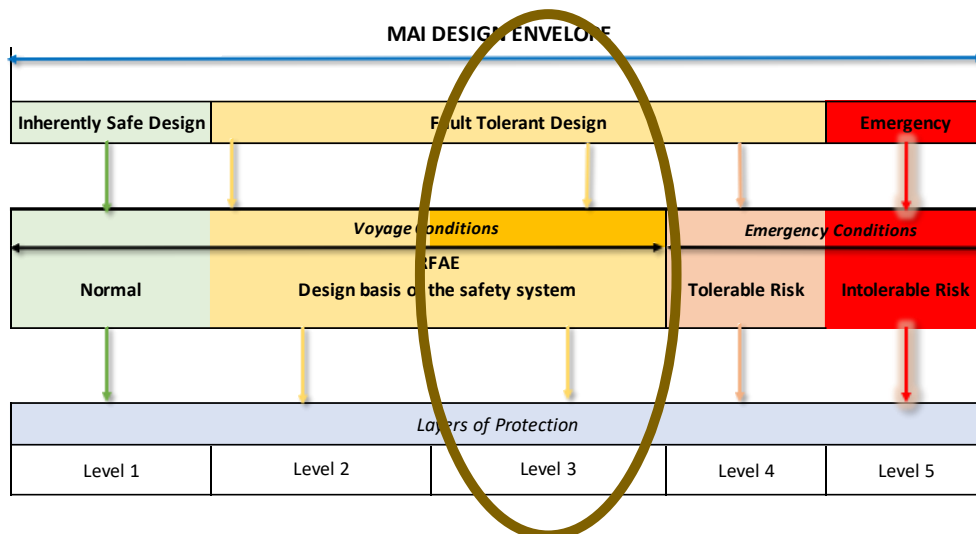


Figure 5-8: Level 3 - Activation of engineered safety features

Level 4 - Limiting consequences and preventing escalation

The fourth layer is intended to limit the consequences of an event and to prevent escalation if the third level of defence does not fully contain the failure. At this stage, the risks remain tolerable and are managed through a combination of automated safety systems and human intervention by qualified and trained staff. These measures work together to prevent further escalation and ensure that the situation does not progress to an intolerable level of risk.

Case 1	<i>onboard crew initiate the release of a gas-based fire-fighting medium and attempt to maintain the vessel functions as far as practicable whilst ensuring the risk do not become intolerable. With no crew on board, the release of a gas-based fire-fighting medium could be quicker as the threat to human life does not need to be considered. Communication with external stakeholders, such as Ship Emergency Response Services [107], will be required during this phase.</i>
Case 2	<i>vessel leaves the area to a place of refuge away from traffic and underwater hazards. An anchor that cannot be recovered could pose a threat to the national infrastructure if it damages data cables, power cables or gas pipelines.</i>
Case 3	<i>use of independent power sources: where an electrical protection device, such as a circuit breaker trips, resetting of the electrical protection devices needs to take into consideration the limitations of the circuit breaker, such as the short-circuit breaking capacity (Icu/Ics) requirements, as defined by IEC 60947 [108].</i>

Table 5-8: Level 4 Scenarios

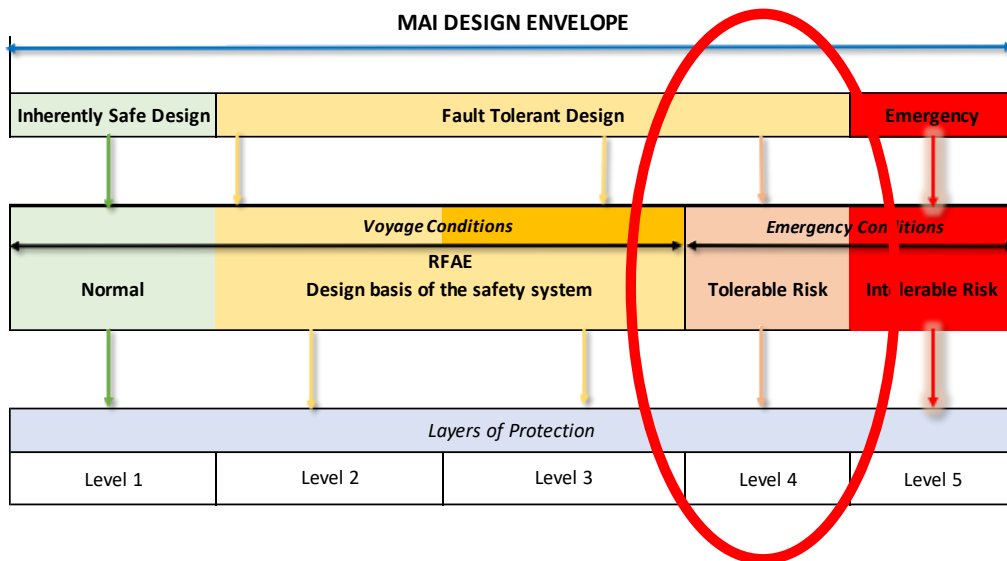


Figure 5-9: Limiting consequences and preventing escalation

Level 5 - Emergency response and external intervention

The fifth layer focusses on responding to the consequences of an event that cannot be contained within the preceding layer. At this level the risks become intolerable and may require external assistance as all other levels have failed to prevent escalation of the event.

Case 1	<i>fire that cannot be controlled by design, or the STCW crew, may require external assistance to be provided, such as attendance of fire-fighting vessels, salvage operations, or land-based emergency services if the risks become intolerable.</i>
Case 2	<i>where the event leads to a vessel drifting and not under command, external assistance may be required, such as attendance of tugs to ensure the risks do not become intolerable.</i>
Case 3	<i>where a total loss of electrical power includes depletion of the emergency sources of electrical power with no means of recovery, external assistance may be required such as attendance of tugs to ensure the risks do not become intolerable.</i>

Table 5-9: Level 5 Scenarios

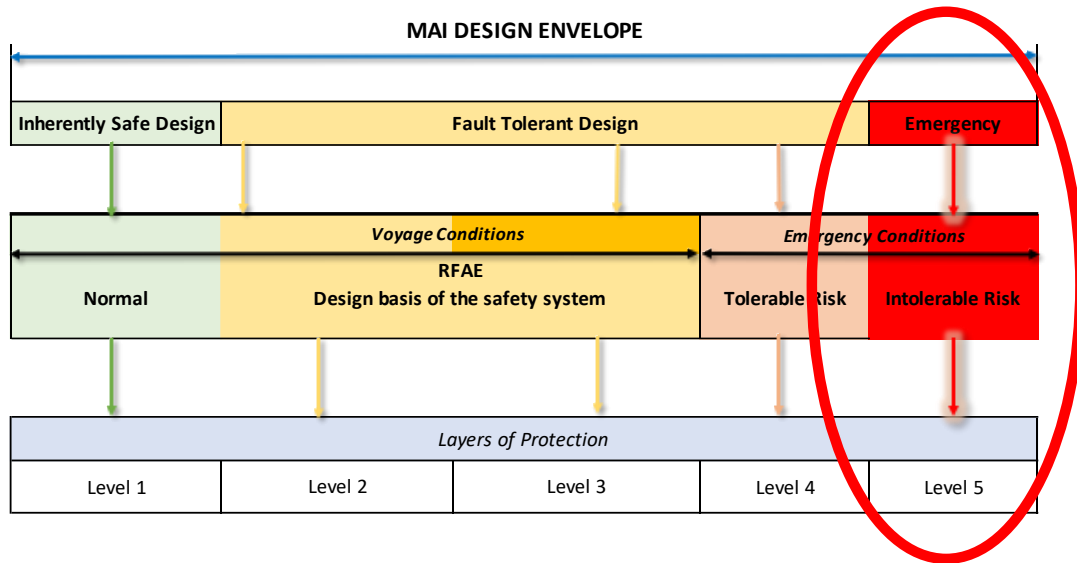


Figure 5-10: Emergency response and external intervention

The absence of a crew [on board a vessel] may result in a rapid escalation towards an emergency condition compared to that of a crewed vessel, primarily because the crew are equipped with the skills and training to respond to incidents. However, the lack of crew can also facilitate the faster deployment of protection systems, as there are no personnel whose safety must be considered before activating such measures. Conversely, when crew and personnel such as service engineers, surveyors etc, are present on board, the activation of protection systems must prioritise the safety of the personnel before deployment which can introduce delays during emergency scenarios.

5.2.9 Fallback State

A 'Fallback State'¹⁸ as defined by ISO23860 is:

'a designed state that can be entered through a fallback function when it is not possible for the autonomous ship system to stay within the operational envelope'.

The IMO provides a similar definition: [109]

'Fallback state means a designed state that can be entered through a fallback response when it is not possible for the MASS with its autonomous or remote-controlled ship functions to stay within the operational envelope'.

The IMO definition extends beyond the physical boundary of the vessel, which aligns with the broader scope adopted in this research. Notably, the IMO refers to a *'fallback response'* rather than a *'fallback function'*, which recognises that such a response maybe compromised of multiple coordinated functions acting together to provide a defined output.

The complexity of any fallback state will be determined by the defined use cases of the MAI, the tolerability of risk acceptable to the owners/company, and the layers of protection provided within the MAI design. Whilst it is not expected that the MAI will recover fully from every fallback state across all identified scenarios, adherence to the ISO's requirement that the fallback states should not result in an intolerable risk. One example is:

- A reduction in active power may be initiated as a protective measure that prevents overheating of a device that limits the rotational speed of an electric propulsion system. While this fallback state is intended to safeguard the propulsion system, it could degrade the vessel's operational capability by reducing the available thrust. Depending on the vessels'

¹⁸ Note 1 to entry: Being in a fallback state should not result in an intolerable risk (frequency and severity of any consequence).

propulsion and steering configuration, such a reduction could adversely affect manoeuvrability, with a potential impact for navigational safety.

- Fallback states that affect essential services, must be assessed in the context of the operational condition of the vessel or vessel functions (manual, remotely controlled, autonomous). For example, a vessel operating in open waters under calm conditions, with minimal surrounding traffic, presents a different risk profile than the same vessel, navigating a congested port environment. In the latter scenario, a loss of manoeuvrability due to reduced thrust could increase the likelihood of a collision taking place.

This example demonstrates that the protection system LoP Level 2 – *Detecting and controlling deviations*, needs to consider the impact on the SoS at the MAI level to ensure the event does not escalate through the MAI-DE levels to an intolerable risk. Accurate identification and management of fallback states under all defined voyage and operational conditions must be considered within the LPM. However, demonstrating the effectiveness of the fallback states will be challenging due to technological advancements and evolving safety, regulatory and stakeholder requirements.

5.2.10 Other Risk Reduction Methods.

Passive safety measures should be incorporated across all elements of the MAI to ensure that no single-point event results in a complete loss of functions required for safety, unless advised otherwise by the relevant stakeholders. Examples of passive safety¹⁹ measures include redundant and independent engine room spaces on a vessel, structural fire protection, and non-slip flooring in the ROCs to minimise accident risks. To achieve an inherently safe²⁰ design passive risk reduction methods must be considered within the hazard analysis. A key challenge is assessing these measures when control is passed between ROC's operating under different legal jurisdictions. Variations in safety regulations, operational standards and oversight requirements may impact the assurance case for the MAI.

¹⁹ Passive safety - Providing and maintaining a safety function without the need for an external input such as actuation, mechanical movement, supply of power or operator intervention.

²⁰ Inherent safety is not the same as 'passive safety'. Where an inherently safe design is not achievable, the design should be fault tolerant'

5.2.11 Overall Safety Requirements Specification

The safety requirements specification will be derived, defined, and agreed upon by the relevant stakeholders. This specification will be informed by the agreed tolerability of risk and be based on the claim of 'Acceptably Safe' under defined operational conditions. Furthermore, it will incorporate fallback states and concept requirements to ensure all elements of the MAI are considered to ensure the risks do not become intolerable.

A key challenge in achieving this lies in the distributed, system-of-systems (SoS) nature of the MAI, which extends beyond a single vessel or operational context. Multiple stakeholders, including regulators, classification societies, technology providers, remote operators, and port authorities, must collaboratively engage in the development of the assurance framework. Additionally, the MAI spans jurisdictions, each with its own regulatory standards, safety expectations, and legal frameworks. These cross-jurisdictional and cross-stakeholder considerations introduce significant complexity in defining, verifying, and gaining acceptance for the safety requirements specification. Combined with the distributed architecture and fragmented regulatory environment, they create a fundamental challenge in establishing a coherent assurance argument that can satisfy all relevant stakeholders.

5.2.12 Overall Safety Validation Planning.

Overall safety validation within the MAI is not a single, discrete activity but a continuous process that evolves across the lifecycle. It is achieved through three interrelated phases — Concept, Demonstration, and In-Service, which together ensure that safety requirements are defined, evidenced, and maintained. These phases provide a structured framework for progressively validating the assurance/safety case, thereby supporting the claim of 'Acceptably Safe' under all defined operational conditions.

The compelling body of evidence presented in the form of an assurance/safety case submitted for regulatory consideration must contain sufficient, coherent and verifiable information to demonstrate that the claims meet the defined objectives and requirements of the MAI. Drawing on best practices adopted from other domains, such as ISO 26262, ARP 4754, and the UK MOD ASEMS [110], the assurance/safety case should present a structured argument supported by clear, traceable claims, and

supporting Body of Evidence (BoE), which covers the defined safety objectives and validates the fallback states proposed for the project.

A key challenge in safety validation planning lies in determining the format and structure of the Body of Evidence (BoE) as well as clarifying the requirements and responsibilities for its development. This raises important questions regarding which stakeholder(s) such as the owners/company, designers, shipyards, or an external third party is/are responsible for developing, compiling and maintaining the single MAI assurance/safety case. Equally important is the question of which regulatory or certification bodies the assurance/safety case must ultimately be submitted to for review and approval/acceptance. Addressing these issues is fundamental to ensuring that the assurance/safety case not only meets technical and safety objectives but also aligns with the complex stakeholder and regulatory landscape that governs the MAI.

It is expected that the development of the assurance/safety case will evolve as the project progresses taking into consideration the unique challenges of the MAI, such as changes to the voyage conditions, operational conditions, regulatory requirements, risks associated with changing crews, owners, or the inability to achieve the layers of protection considered during the initial risk assessment of the MAI.

The development of assurance cases is well documented, as shown in [111] [112] [113], as such this research does not propose a new model but rather builds upon these established approaches. Nevertheless, there are several critical steps within the development of an assurance/safety case that require careful consideration. One of these steps involves the activities carried out during the Concept Phase, described in the following section.

5.2.12.1 Concept Phase Assurance/Safety Case.

During the Concept Phase, detailed technical specifications and system architectures may still be under development. Consequently, risk identification must be conducted primarily on a functional basis for the MAI, taking into consideration the intended operational conditions of the MAI and the broad range of potential stakeholders involved. By the conclusion of this phase, the project should have established a preliminary safety strategy derived from the outputs of the SPM and the MAI-DE. This strategy must demonstrate that the fundamental safety requirements defined in Section 5.2.11 are understood and that the assurance/safety case management structure is in place.

It is anticipated that several uncertainties or partially defined requirements will remain at this. Where assumptions are made, these must be clearly documented, including their rationale, potential impact, and a strategy for validation or revision in later lifecycle phases. This approach ensures traceability of risk and assumption management throughout the lifecycle and supports the adaptive development of the assurance/safety case in line with the principles of the LPM.

5.2.12.2 Demonstration Phase Assurance/Safety Case.

This stage plays an important role in confirming that the MAI can operate within an acceptable level of operational risk under real-world or representative conditions. At this stage, the assurance/safety case must evolve from abstract safety arguments to include evidence-based demonstrations that the proposed system functions and fallback states perform as intended under both normal operations and reasonably foreseeable abnormal scenarios. In practice, simulation can be vitally important in generating the Body of Evidence (BoE) and in meeting pre-operational requirements, particularly when real-world testing is constrained or impractical.

The SPM should inform development of a verification and validation strategy that clearly defines how the safety requirements will be demonstrated to the relevant stakeholders, including the criteria for acceptance. This strategy should also establish the appropriate balance between simulation-based and real-world testing to ensure credible and robust safety assurance.

Furthermore, the Assurance/Safety Case should:

- Clearly assign safety responsibilities across stakeholders, particularly where system control is distributed between shipboard systems, ROC's, and communication infrastructure.
- Contain sufficient instructions, guidance, training and resource requirements to ensure that all relevant stakeholders understand and can fulfil their roles.
- Demonstrate that the system is maintainable, inspectable, and recoverable in line with the MAI operational requirements and fallback expectations.
- Include results of independent assessments or audits, where applicable, to strengthen credibility and satisfy regulatory expectations.

The Demonstration Phase should therefore be viewed not as a stand-alone activity but as a pivotal lifecycle milestone that validates the operational readiness of the MAI. It ensures that the system can

perform within the defined operational envelope and demonstrate that the claim of ‘Acceptably Safe’ can be satisfied.

5.2.12.3 In Service Assurance/Safety Case.

This will be developed to support the introduction of the MAI into service. It will need to demonstrate how the assurance/safety case will be maintained throughout the life of the MAI, taking into consideration any changes to regulations, the introduction of new crews, a change of flag, a change of voyage plan or new owners, all of which may result in changing requirements that if not considered could result in the risks becoming intolerable. It will be left to the stakeholders to identify further steps in the development of the assurance/safety case, noting the dynamic nature of the MAI.

5.2.13 Operate Maintain Diagnose and Repair (OMDR).

Where requirements to operate, maintain, diagnose, and repair the MAI are specified, the associated risks must be identified and assessed within the LPM and the SPM. When human intervention is required, it is essential to define the necessary competencies and training requirements. In 2019, it was observed that *“the competency framework [for remote operators] is yet to be develop”* [114]. More recently, the UK Maritime and Coastguard Agency (MCA) addressed this issue in MGN 703 (2024), which provides information on training and competence for Remote Operators of Remotely Operated Unmanned Vessels (ROUVs) certified under the Workboat Code Edition 3 [115]. Additionally, the IMO is actively considering this matter through its Sub-Committee on Human Element, Training and Watchkeeping.

The absence of a unified framework for operator competencies can pose significant safety challenges. For example, a change in the location of a ROC could result in different competency requirements for the ROC operators, as defined by the national regulators in that jurisdiction. Additionally, all relevant personnel must be able to effectively isolate or verify the isolation of autonomous or remotely controlled functions, which is critical for ensuring the safety of personnel interacting with the MAI systems.

Given that the MAI can transition between operational conditions (*Manual, Remote Control, Autonomous*) due to legal, technical or company procedures, the allocation of function between the

human and the technology must be explicitly considered within the LPM. Similarly, any changes in the voyage conditions (*Normal, Reasonably Foreseeable Abnormal, Emergency*) must be evaluated to ensure the human role within the MAI, especially during remote control of a function is properly accounted for, as a failure to do so could quickly result in the risk(s) becoming intolerable. As stated in [65], the authors assert that:

“The requirement to operate must ensure the risks do not exceed the benefits, and the possibility of meaningful control exists. Consideration shall also be given to designing ethically defensible systems”.

This principle is particularly relevant when humans are required to carry out maintenance activities that necessitate human presence alongside autonomous operations. The isolation of the autonomous functions must be both verifiable and validated by the relevant stakeholders. This requirement must be explicitly considered within the LPM (Figure 5-1) and the SPM (Figure 5-4) to ensure the risks do not become intolerable.

5.2.14 System Disposal and Transition Management in the MAI Lifecycle.

The disposal or replacement of system or sub system within the MAI requires a structured approach to ensure the requirements of the assurance/safety case and safety requirements are maintained throughout the MAI lifecycle.

In the maritime sector, replacing hardware does not happen very frequently due to extended warranties for material and workmanship. However, vessels can be designed for a 30-year lifecycle or longer, an example of this in HMS Hermes laid down in 1944. The ship remained in service with the Royal Navy until 1984 and remained in service with the Indian Navy until 2017, 63 years after being laid down. Over this time, the operational requirements and onboard technologies evolved significantly, particularly in terms of the aircraft the vessel supported which were significantly different from those available in 1944. This necessitated system upgrades to maintain operational relevance [116].

For the MAI, we can expect software changes to take place throughout its lifecycle, this may include system improvements, error correction, enhanced protection against cyber-attacks, or changes to risk mitigation processes based on the stakeholder's tolerability of risk.

To ensure the risks do not become intolerable, a software quality assurance processes shall be considered within the LPM (Figure 5-1) and the SPM (Figure 5-4) and applied by the company to ensure the risks do not become intolerable. Although this is a standard practice and standards such as ISO 9001 [117], ISO9003 [118], and ISO/IEC 25000 [119], provide a robust framework, the requirement to demonstrate compliance will be the responsibility of the relevant stakeholders, such as the manufacturers and the company/shipowner.

Beyond digital and physical system disposal, personnel transitions can present additional safety considerations. A notable example occurred on the 17th March 2022, when the shipping company P&O Ferries replaced the complete crew of the vessel, which resulted in the vessel being detained by the regulatory authority, the MCA. [120]. Their report stated: *"The Pride of Kent has been detained due to failures on vessel documentation, crew familiarisation and training, and emergency equipment not functioning properly, indicating a failure of the implementation of a safety management system"*.

This case highlights the essential role that personnel competence, training and effective handover procedures play in maintaining operational safety. Additionally, the MAI introduces an added layer of complexity when transfer of control is required, particularly where multiple ROC's and remote operators are involved. Transferring control between different remote operator, remote operator workstation or other ROCs present specific risks that are unique to the MAI. For example, a handover between two ROCs may result in a temporary loss of situational awareness if system states, sensor data, or navigational information are not synchronised in real time. Such discontinuities can lead to delays in decision-making or conflicting control inputs, thereby increasing the likelihood of an event escalating beyond tolerable limits. These risks are not explicitly addressed under the current requirements of the STCW Convention, which does not consider remote operations or the roles and responsibilities of remote operators.

5.2.15 Summary

Chapter 5 introduced a Lifecycle Process Model (LPM) for the Maritime Autonomous Infrastructure (MAI), that provides a structured, coherent, and traceable decision-making framework. While presented linearly, the LPM is deliberately adaptive and iterative, accommodating dynamic voyage and operational conditions, evolving regulatory requirements, and changing stakeholder expectations. This adaptability is a core design choice: it recognises that safety assurance for crewless or remotely controlled operations must be continuously assessed as context of use shifts.

A central theme is ‘bias control’ in the assurance/safety case. This chapter argued that prescriptive evidence common to conventional vessels cannot simply be imported into the MAI context. By explicitly seeking both affirming and non-affirming evidence, and by introducing the requirement for an ISA to be carried out using an ISAP, the chapter replaces confidence by tradition with evidence-led credibility, mitigating institutional and cognitive biases that could undermine claims of ‘Acceptably Safe.’

Technically, the chapter distinguished inherently safe design and fault tolerance as complementary, rather than interchangeable principles, shifting the focus of safety from procedural response to design-time prevention and verifiable fallback.

The chapter’s unique methodological contributions are: the development of Safety Process Model (SPM), which provides the structured means to derive, assess, verify, and consolidate safety requirements into a compelling body of evidence; the Layers of Protection (LoP) developed for the MAI, explicitly compensating for the removed human intervention layer; and the MAI Design Envelope (MAI-DE), which integrates concept, voyage conditions (normal/RFAE/emergency), and LoP to define an operational safety boundary and thresholds for intervention. Together, the application of the LPM, SPM, MAI-DE and LoP models within this thesis demonstrate their utility as a structured and context-aware methodology for risk identification, assurance development, and system integration within the MAI.

Accordingly, the effective application of this methodology depends on clarifying institutional and operational roles that shape its evidence base. This is achieved through stakeholder and actor analysis, a foundational activity that structures subsequent analysis and validation by distinguishing stakeholders (influence on requirements and tolerability of risk) from actors (direct control and interaction with MAI functions).

The chapter recognised that operating across-domains and jurisdictions introduces material legal, organisational, and operational challenges. These challenges include conflicting statutory duties, divergent assurance and evidence thresholds, along with fragmented duty-holder accountability. To address these issues, the chapter recommends a phased and iterative approach to stakeholder engagement, allowing strategies to be revisited and refined as circumstances evolve. It also emphasises the importance of explicitly allocating responsibility and accountability, ensuring that each party's role is clearly defined and grounded in demonstrable authority and capability.

The chapter also formalised safety across the lifecycle, including Voyage Planning (normal/reasonably foreseeable abnormal/emergency), Operational Conditions (manual/remote/autonomous) and their transitions, Hazard and Risk Analysis with multi-domain participation, Fallback States, OMDR (with competence/isolation emphasis), and Disposal. The staged validation plan emphasises configuration control of the evidence and clarity on ownership of the single assurance/safety case.

Within the SPM, 'Legal' and 'Human-Centred Design' are treated as influencing interfaces. By contrast, responsibility, accountability allocation (grounded in demonstrated authority and capability), contractual and liability models across jurisdictions, and through-life Human-Centred Design are identified as future work. Stating these inclusions and exclusions strengthens the credibility of the claims made in Chapter 5.

In summary, Chapter 5 presented a rigorous, design-led, evidence-oriented assurance methodology for the MAI that renders the 'Acceptably Safe' claim testable under dynamic operational conditions. The chapter's clarity on what is delivered versus what is reserved for future work provides a defensible foundation for regulatory dialogue and subsequent research.

Chapter 6 : Application of the LPM.

This chapter presents a series of case studies to demonstrate the practical application of the Lifecycle Process Model in defined operational scenarios. The selected use cases encompass both crewed and uncrewed maritime operations, including functions conducted remotely from a Remote Operations Centre, as well as those performed autonomously. Each case study applies the LPM to identify, assess and address the risks throughout the complete lifecycle process. These examples serve to illustrate how the LPM supports structured decision making, promotes safety assurance and facilitates the development of the compelling body of evidence and demonstration of 'Acceptably Safe' in the context of the MAI.

6.1 Case Studies.

The LPM was used to assess the selected use cases in the context of both crewed and uncrewed operations, including remote control and autonomously operated functions. The assessment considered potential risks at various stages of the LPM, with particular attention to those that could result in a non-compliance against a statutory instrument or escalate to an emergency condition in a relatively short period of time.

As illustrated in Figure 5-2 – '*interdependencies between the stages of the LPM*', the assurance/safety case is influenced by several independent factors, including the **Operational Conditions** (*Manual, Remote Control, Autonomous*), the **Stakeholder Requirements** and **Voyage Conditions** (*Normal, Reasonably Foreseeable Abnormal, Emergency*). Additionally, within a single voyage, the stakeholder requirements may change, further impacting safety and regulatory compliance. As an example: the port authorities may require the ship to be diverted, this would need the risks to be evaluated to ensure they remain tolerable. Where a vessel cannot meet the new requirements the **layers of protection** and **fallback state** would need to be applied, this may involve the need for external assistance if there are no crew on board

Use Cases 1 and 2 represent basic vessel functions commonly performed at sea, while Use Cases 3 and 4 highlight unique challenges specific to remote or autonomous operations. Each case has been evaluated using the LPM to assess its implications for safety and regulatory compliance:

1. **Operation of the Navigation Lights** – evaluated to demonstrate compliance with COLREGS.
2. **Anchoring** – A function that maybe required by the regulatory authorities or through necessity.
3. **Abandonment of a land-based ROC** - Addressing contingency measures for ROC failure or abandonment.
4. **Loss of Situational Awareness (SA)** – Analysis of the risks associated with degraded modes of operation leading to a deterioration or failure to achieve the required level of situational awareness in a defined context of use. The loss of SA could quickly result in an intolerable risk occurring based on the stage within the voyage plan e.g. congested waters/berthing or pilotage conditions.

Use Cases 3 and 4 are particularly important within the context of maritime autonomy. Use Case 3, which addresses the abandonment of a land-based Remote Operations Centre (ROC), introduces challenges specific to remote and autonomous operations, where traditional shipboard crew responses are not available. Ensuring that contingency measures and fallback states are robust in these scenarios is essential to maintain control and to mitigate safety risks associated with ROC failure.

Use Case 4, focused on the loss of situational awareness (SA), is equally critical for autonomous or remotely controlled functions, as situational awareness is typically maintained by an onboard crew in conventional operations. In an autonomous or remote-control environment, a degradation or failure in SA can quickly escalate into an intolerable risk, especially in high-risk areas such as congested waters or during pilotage and berthing operations. The evaluation of these use cases not only highlights the specific challenges of autonomous or remote operations but also reinforces the need for systematic validation of more conventional vessel functions within the MAI framework.

6.1.1 Use Case 1: Operation of Navigation Lights.

Traditionally, navigation lights have been activated manually by the officer in charge of the navigational watch, with manufacturers providing operational guidance to ensure correct activation of the lights as required by COLREGS, with verification typically performed by visual means. To support compliance, integrated audible alarms are included at the control station to alert the crew in the event of lamp failure or when luminous intensity degrades below manufacturer-recommended thresholds (e.g., for LED-based systems). In addition, visual indicators and manual changeover mechanisms are provided to enable the crew to address lamp failures directly.

Where a remote operator is responsible for the control of navigation lights, assurance of correct light status is dependent on the availability of the communication link between the vessel and the ROC. In the event of a communication loss, the ROC operator would be unable to fulfil the requirements of COLREG Rule 3, which includes taking appropriate action to avoid collision. Under such conditions, the vessel would be classified as Not Under Command (NUC), necessitating the activation of appropriate lights and day shapes.

This illustrates the need to consider the MAI as an integrated SoS in which function allocation, including fallback states during loss of connectivity must be systematically defined. For example, a loss of communications for a duration exceeding a pre-defined threshold, considered as a RFAE should trigger autonomous functions on the vessel activating the lights and deploying the day shapes for NUC. This illustrates the need to consider integrated design requirements and the need to analyse the vessel, the ROC and communications systems within the LPM to ensure that no single point of failure could compromise navigational safety.

A typical arrangement of navigation lights is shown in Figure 6-1 where the light fittings are mounted on a vessel in accordance with the requirements of COLREGS Annex 1 – *Positioning and Technical Details of Lights and Shapes*. The stern light arrangement shown in the centre panel of Figure 6-1 consists of two vertically mounted fittings²¹, with one active and one on standby in the event of a

²¹ 'Sternlight' means a white light placed as nearly as practicable at the stern showing an unbroken light over an arc of the horizon of 135 degrees and so fixed as to show the light 67.5 degrees from right aft on each side of the vessel.

failure of the main light. The lights located on top of the stern mast are ‘all round lights’²² which are displayed as required in accordance with the requirements of COLREGS.



Figure 6-11: Arrangement of Navigation Lights

Navigation light arrangement Stern light arrangement – Navigation light control panel
Images courtesy of Warstila and MarLog

The navigation light and monitoring control panel is normally located on the bridge of the ship, providing the master or delegated authority with immediate access to activate the lights as required by COLREGS – Rule 20 Application (b)²³. In the event of a primary navigation light failure, the system is designed to issue both audible and visual alarms to alert the navigating personnel, thereby enabling prompt activation of the secondary light to maintain compliance with COLREGS.

When this panel is located within a ROC, the responsible operator is expected to respond in a manner equivalent to that of a crewed vessel. However, a critical distinction arises in the verification process as confirmation of the secondary light activation is entirely dependent upon the connectivity being available between the vessel and the ROC. Consequently, any disruption in connectivity introduces a potential risk to compliance with the navigation light requirements under COLREGS.

²² ‘All-round light’ means a light showing an unbroken light over an arc of the horizon of 360 degrees.

²³ Rule 20 Application (b). The Rules concerning lights shall be complied with from sunset to sunrise, and during such times no other lights shall be exhibited, except such lights as cannot be mistaken for the lights specified in these Rules or do not impair their visibility or distinctive character, or interfere with the keeping of a proper look-out

Analysis

By applying the principles outlined in the LPM (Figure 5-1) several risks were identified when the vessel is operating with no crew on board. Key findings highlighted the reliance on connectivity solutions to verify the functionality of the lights and the inability to perform basic maintenance, such as lamp replacement or control system diagnostics. Table 6-1 provides a comparative analysis of navigation light operations across a crewed, uncrewed remotely operated, and autonomous MAI.

Table 6.1: Operation of Navigation Lights			
Scenario	Crewed Vessel	Remotely Controlled Function - Crewless	Autonomous Function - Crewless
Normal operation of the navigation lights	STCW-trained crew will manually switch on the navigation lights at the control panel and verify that they are working, through a combination of visual verification or by responding to any alarm indicating that a lamp has failed.	Design must incorporate measures to mitigate risks associated with single-point failures. This now extends to the power supply requirements of the Remote Operations Centre (ROC) to ensure compliance with regulatory requirements for navigation lights. (COLREGS). Additionally, the activation of the navigation lights will be carried out by ROC-trained operators. Verification will rely on connectivity being available between the ROC and the vessel.	In the event of a navigation light failure, onboard system(s) will autonomously switch to standby light without human intervention. Both the activation and continuous monitoring of the navigation lights will be managed through the onboard autonomous systems.

Table 6.1: Operation of Navigation Lights			
Scenario	Crewed Vessel	Remotely Controlled Function - Crewless	Autonomous Function - Crewless
RFAE (Fault tolerant). Lamp failure	<p>In the event of an alarm indicating a lamp failure, the trained crew will respond by activating the manual changeover switch and verifying the functionality of the replacement lamp.</p> <p>Additionally, the onboard crew can replace the faulty lamp or unit in accordance with the manufacturer's recommendations to fully restore the redundancy requirements of the navigation light system.</p>	<p>The ROC trained operator will respond to an alarm in the event of a failure of the navigation lights.</p> <p>System resilience may require multiple light sources to ensure a single point event does not result in the loss of the function.</p> <p>Repairs to a failed light cannot be made until personnel attend on board the vessel. The ROC power supply arrangements should satisfy the requirements of SOLAS. If the ROC power supply fails, the repair should be carried out by qualified personnel which may require land-based certification.</p> <p>Verification and validation that the lights are functioning will depend on connectivity between the vessel and the ROC.</p>	<p>On a crewless vessel, the failure of a single navigation light should not result in the complete loss of function.</p> <p>Automated alert systems could be implemented to advise vessel operators/ company personnel, or maintenance teams of a failure, enabling prompt intervention when feasible.</p>

Table 6.1: Operation of Navigation Lights			
Scenario	Crewed Vessel	Remotely Controlled Function - Crewless	Autonomous Function - Crewless
Emergency – incorrect or absent display of navigation lights.	<p>If a crewed vessel is unable to display the correct navigation lights due to a failure, lack of spare parts or the inability to replace a faulty lamp or fitting under adverse environmental conditions, alternative risk mitigation measures must be implemented.</p> <p>If the environmental conditions improve, the crew may repurpose rarely used operational lights to temporarily restore compliance with COLREG requirements until proper repairs can be conducted.</p> <p>The crew can notify nearby vessels and maritime authorities of a non-compliance, to maintain situational awareness and prevent potential navigational hazards.</p> <p>These interventions help ensure that risks associated with navigation light failure remain within tolerable limits.</p>	<p>Incorrect or absent display of navigation lights presents a significant hazard to navigation, increasing the likelihood of collisions and potentially creating an intolerable safety risk.</p> <p>Regulatory authorities may enforce operational restrictions on vessel, including prohibiting sailing until compliance is restored.</p> <p>For a crewless vessel, failure to activate or verify functionality of navigation lights may result from various factors, including:</p> <ul style="list-style-type: none"> a) Loss of connectivity between the vessel and the ROC. b) Abandonment or malfunction within the ROC. c) A cyber-attack preventing control of the navigation lights. d) Operator failing to adhere to required procedures <p>Given the criticality of the navigation light functionality and its impact on safety, the principles of an inherently safe design as defined within the LPM, should be considered at the concept phase within the MAI design.</p> <p>Additionally, a defined ‘fallback’ state should be implemented to ensure the risk remain tolerable.</p> <p>This approach may necessitate autonomous operation of the navigation light functions to ensure risks do not become intolerable & demonstration of ‘Acceptably Safe’ is achieved.</p>	<p>Failure to display the correct navigation lights must be promptly communicated to relevant stakeholders and nearby vessels to ensure situational awareness and mitigate potential navigational risks.</p>
See Figure 5-1 – Voyage conditions, Overall safety requirements, Fallback state, Layers of Protection, Hazard and risk analysis, Tolerability of risk, Overall safety validation.			

Table 6-1: Operation of Navigation Lights

The objective of Stage Gate 1 is to confirm that the remote operation of the navigation lights remains compliant with the requirements of COLREGS. This includes adherence to the electrical power supply requirements defined by the regulatory authorities. In cases where these requirements cannot be met, the decision to proceed with the design or implement modifications is a decision to be made by the relevant stakeholders, noting that a non-compliance of the statutory requirements, could have safety and legal implications

For navigation lights, a loss of connectivity—classified as a reasonably foreseeable abnormal event, could prevent verification of compliance with COLREGS

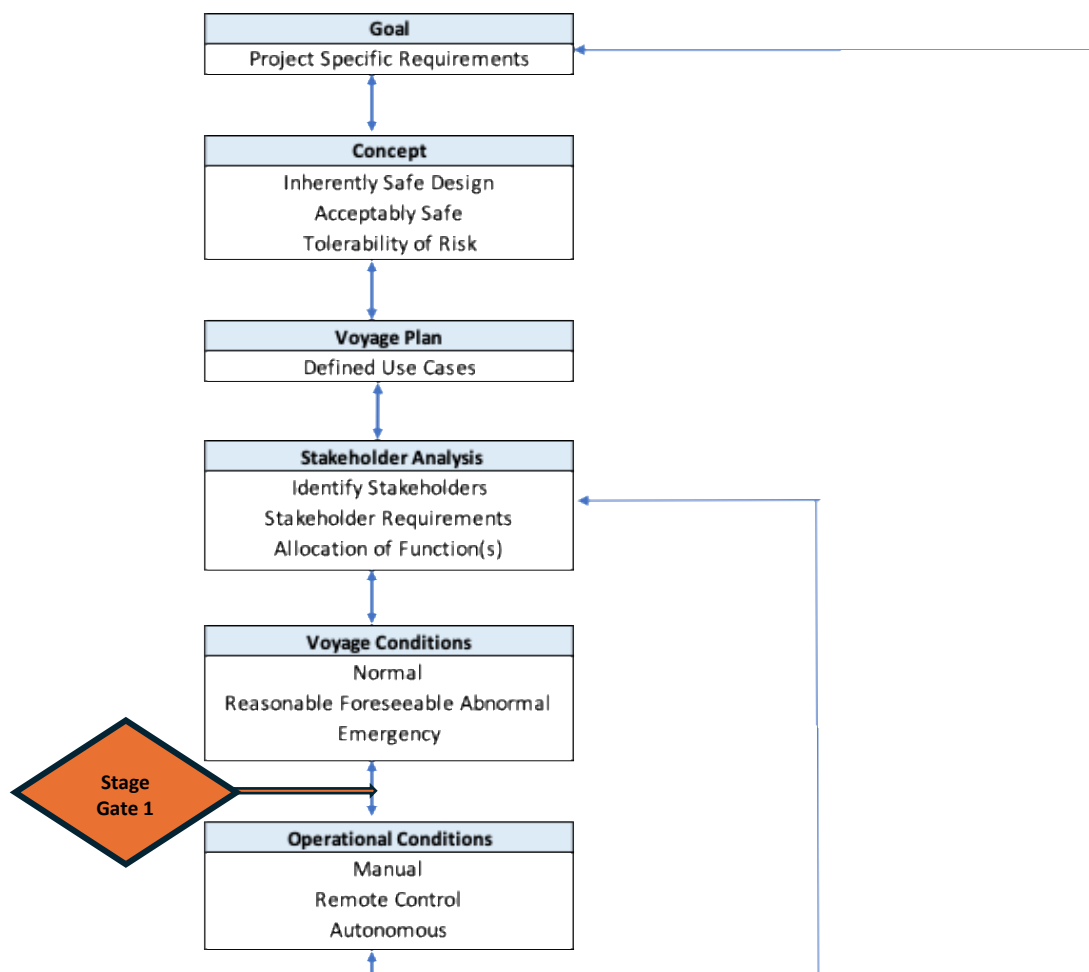


Figure 6-12: Operation of Navigation Lights Stage gate review

The stage gate evaluation should consider all possible failure modes, such as demonstrating compliance with the power supply requirements for navigation lights: SOALS which stipulate that:

‘the navigational lights and other lights required by COLREGS to be supplied with an emergency source of electrical power’.

A further requirement exists where the emergency source of electrical power is a generator to provide a:

‘transitional source of emergency electrical power’, that will supply the navigation lights as required by COLREGS.

Although the ROC does not directly supply power to the navigation lights, regulatory requirements influence the design of the electrical power systems within the ROC and the communication network. The overarching intent of SOLAS for navigation lights can be interpreted as ***‘no single point event should result in the complete loss of the function’***, which in this case, is the vessels inability to display the navigation lights as required by COLREGS. To comply with the prescriptive requirements of SOLAS the electrical power supply must consider common cause failure, such as the main and emergency source of electrical power being provided from the same electrical sub-station.

The analysis further indicates that the resilience of remote operation of the navigation lights introduces new risks, such as latency, and data transmission failure, is dependent on all elements of the MAI, and not just the vessels systems,

6.1.2 Use Case 2: Anchoring.

Anchoring is a maritime process that secures the vessel to the bed of a body of water to prevent the vessel drifting due to wind or current. As defined by Skuld [121], anchoring is:

‘a critical operation on vessels, and an improper anchoring procedure could cause damage and loss to the vessel, other vessels, property, and the environment. The consequential losses of grounding and collision due to anchor dragging or loss can be significant’

Anchoring is a complex and challenging process and requires the expertise of the master and crew, good bridge management, anchor planning, risk assessment, anchor watchkeeping, and clear communication between all relevant stakeholders to be in place for successful anchor deployment and recovery. Anchoring operations are undertaken for several reasons, such as:

- awaiting a berth,
- awaiting suitable tides before proceeding,
- availability of the cargo,
- awaiting orders,
- a requirement by the port authorities,
- maintaining a position to allow repairs to be carried out.

Similarly, anchor retrieval may be necessary due to port authority instructions to vacate the anchorage or in response to the anchor dragging, which necessitates prompt corrective action to prevent navigational hazards. A typical arrangement of the anchoring and mooring equipment is shown in Figure 6-3.



Figure 6-13: Anchoring and Mooring equipment
Images courtesy of McGregor and Bulutlu marine.

The challenge in deploying and recovery of an anchor is the identification of the risks when there are no crew on board the vessel. The LPM and SPM were used to identify the potential risks, examples of which are included in Table 6-2.

Table 6-2: Anchoring Operations			
Scenario	Crewed Vessel	Remotely Controlled Function	Autonomous Function - Crewless
Normal operation of anchoring equipment.	<p>STCW on-board trained crew will operate anchoring equipment in accordance with the anchor plan and instructions from the master.</p> <p>Communications between the bridge team and anchoring team is essential for safe anchoring. Any issues such as the anchor dragging, or entanglement of the anchor chain will be immediately advised to the master.</p> <p>Verification of activities such as removal of the sea fastenings, sternway speed and confirming there are no obstructions below the anchor (such as a tug) will be required before the anchor is dropped.</p> <p>Anchor watches will be carried out by the STCW crew.</p>	<p>ROC trained crew will be responsible for releasing the anchor based on verified data received from the vessel.</p> <p>Verification of location of the vessel, release of sea fastenings, sternway speed and confirmation that no obstructions exist under the anchor will be required before the anchor is released.</p> <p>Communication between the ROC operators and the relevant authorities must be confirmed before anchoring takes place.</p> <p>Anchor watches will be carried out by the ROC operators using onboard and off board technologies.</p> <p>Anchor dragging or entanglement issues would need to be considered in the risk analysis and appropriate fallback states would need to be agreed with the relevant regulatory authorities.</p>	<p>Conditions for achieving an inherently safe design would have been identified by following principles within LPM (Fig 5-1) & SPM (Fig 5-4).</p> <p>If a relevant authority requires vessel to anchor, a means of transmitting this command to the vessel and verifying its receipt will be required.</p> <p>Autonomous functions should process all relevant anchoring information and activate the anchoring system accordingly. A similar process should be followed for recovering the anchor.</p> <p>Concept & requirements of 'Anchor Watches' will need to be redefined to align with autonomous operations.</p> <p>Where anchoring is deemed unnecessary, any risks associated with this decision should be identified and agreed upon by all relevant stakeholders.</p> <p>Additionally, fallback states must be clearly defined, verified, & validated to ensure safe operations under defined operational conditions.</p>

Table 6-2: Anchoring Operations			
Scenario	Crewed Vessel	Remotely Controlled Function	Autonomous Function - Crewless
<p>RFAE – Anchor chain twisting.</p> <p>Other potential RFAE's to be derived, but can include:</p> <p>Anchor dropped in restricted area.</p> <p>Anchor dropped when ships sternway speed is too high.</p> <p>Anchor dropped on another vessel.</p> <p>Hand-over procedures between watches inadequate.</p>	<p>Procedures for recovery of a twisted anchor chain during recovery would require effective communication between the bridge and the anchoring team.</p> <p>The on board STCW crew can take appropriate action through control of the anchoring system, visual observation, and communication with the bridge team who will be managing control of the propulsion and steering systems. Where required, the crew can provide manual intervention to raise and secure the anchor.</p>	<p>The procedures for recovering a twisted anchor should include visual feedback from the anchoring system, the anchor chain, anchor position, ensuring the remote operator has comprehensive situational awareness.</p> <p>Additionally, the remote operator should receive detailed and validated data on the anchoring system's status and performance, such as chain tension, deployment length, and operational diagnostics.</p>	<p>The procedures for recovery of an anchor chain that is twisting would require data to be provided to the onboard system for it to make an informed decision on the course of action to recover the anchor. This could include visual data, external lighting, information from the anchoring automation system, propulsion and steering systems.</p>

Table 6-2: Anchoring Operations			
Scenario	Crewed Vessel	Remotely Controlled Function	Autonomous Function - Crewless
Emergency – unable to recover the anchor – requires disconnection of the bitter end.	STCW staff can remove the bitter end pin allowing the anchor to fall away from the vessel. Verified by visual observation, sound and a big splash.	<p>The vessel's design should include a method for disconnecting the anchor chain.</p> <p>The inability to disconnect the anchor chain could escalate into an emergency condition.</p>	<p>If the vessel begins drifting or dragging within a restricted area, could potentially result in an intolerable risk.</p> <p>The autonomous functions could be arranged to automatically request external assistance to ensure the risks remain tolerable.</p> <p>For consideration, if external assistance is required, the collision avoidance system may need to be disabled to allow the assistance vessel to approach.</p>
See Figure 5-1 – Voyage conditions, Fallback state, Layers of Protection, Hazard and risk analysis, Tolerability of risk, Overall safety requirements, Overall safety validation.			

Table 6-2: Anchoring Operations

On a crewed vessel, the STCW crew manage the release of the sea fastenings, lowering and recovery of the anchor, and resolution of events such as a twisted anchor. The master of a ship must arrange for an appropriate and effective watch to be maintained for the purposes of safety as required by Reg 57 and Section A-VIII, part 5 of the STCW Code (watchkeeping in port). When a reasonably foreseeable abnormal event takes place, such as the sea fastening requiring 'physical attention' before they are released, the crew ensures that the risks remain tolerable.

On crewless vessels, where sea fastening removal relies on remote or autonomous operations, a failure to release the fastenings could prevent anchor deployment, potentially leading to an emergency scenario.

- the claim of 'Acceptably Safe' under varied operational and voyage conditions. This use case reinforces the necessity of collaborative stakeholder engagement in defining acceptable fallback states, validating system autonomy boundaries, and ensuring that layered protection measures are tailored to both normal and degraded modes of operation.
- Ultimately, anchoring, though historically routine, emerges as a complex SoS challenge within the MAI. It exemplifies the broader argument of this thesis: that successful deployment of maritime autonomy or remote-control functionality demands not only technological capability but also a rigorous, dynamic, and stakeholder-informed assurance process.

6.1.3 Use Case 3: Emergency Condition Fire within a land-based ROC.

The scenario presented in this use case, is a unique event for the MAI, wherein the term ‘disabled’ refers to the evacuation of a ROC due to a local emergency, e.g. a fire alarm within the ROC requiring all personnel to immediately vacate the space in compliance with company safety procedures, with re-entry permitted only upon authorisation from the land-based emergency services (e.g. fire brigade). Table 6-2 illustrates the implications of such an event by comparing its impact across crewed and crewless operation of a vessel operations and considers the impact of the event on the safety of the personnel, the vessel and the environment.

Unlike conventional maritime emergencies that originate at sea, this case involves an external disruption to the control environment, which can have critical implications for the continued safe operation of a crewless vessel when its functions are being remotely controlled. A fire alarm within the ROC may require immediate evacuation of personnel in accordance with occupational safety protocols, thereby disconnecting the human-machine interface essential for remote control. It is expected that ROC evacuations will be carried out through routine fire drills in accordance with the company’s safety procedures. These drills provide an opportunity to test and verify the fallback state applicable to the MAI, ensuring that the system risks remain tolerable even in the absence of human intervention.

This event highlights a fundamental shift in risk allocation, wherein safety no longer depends solely on shipboard systems, but also on the agreed fallback states resilience of a land-based control infrastructure. As such, this use case offers a critical analytical framework for evaluating fallback states, function allocation, and the layers of protection required to maintain the vessel within tolerable risk thresholds under degraded or emergency conditions.

Table 6-3 - Fire in a Land-Based ROC

Scenario	Crewed Vessel	Remote Controlled Function – Crewless Vessel	Autonomous Fn - Crewless
Evacuation of the ROC	<p>No impact on safety of vessel as event is contained within ROC.</p> <p>ROC used for monitoring purposes only.</p>	<p>The ability to maintain control of the vessel functions could be compromised if the ROC is abandoned. Arrangements should be made to maintain human control/interaction of the functions, or the function reverts to autonomous operation.</p>	<p>No impact on safety of vessel as event is contained within ROC.</p> <p>Ability to intervene or monitor the vessels functions could be compromised</p>
Fallback State	<p>No impact on safety of the vessel as the event is contained within the ROC</p>	<p>Fallback state must account for scenarios where the operator cannot control the vessel due to a loss of access to the control or safety systems within the ROC. The time required to re-establish control may depend on land-based emergency services granting access to the facility, which can vary based on the ROC's location.</p> <p>If a transfer of control to another ROC is possible, the procedures for verification and control transfer must be clearly defined. Additionally, the legal implications of such a transfer should be thoroughly understood by all relevant stakeholders.</p> <p>Where transfer of control to another human is not possible, could the system revert to fully autonomous mode?</p> <p>Where a vessel is not under command (NUC) due to a fire in the ROC, the visual signals as required by COLREGS would need to be activated autonomously.</p>	<p>No impact on safety of the vessel as the event is contained within the ROC.</p>

Table 6-3 - Fire in a Land-Based ROC

Scenario	Crewed Vessel	Remote Controlled Function – Crewless Vessel	Autonomous Fn - Crewless
Vessel is in port.	No impact on safety of the vessel as the event is contained within the ROC.	<p>Personnel onboard a vessel when in port, such as dock workers, maintainers, surveyors or port state control inspectors must be promptly informed if the remote control of the vessel's functions has been compromised.</p> <p>Clear and immediate communication protocols should be established to ensure their safety in the event of a ROC failure or operational procedure that has an impact on control of the vessel's functions.</p> <p>Failure to notify all relevant stakeholders could lead to unacceptable safety risk.</p> <p>Fallback state must be clearly defined, agreed upon by all stakeholders, & supported by unambiguous emergency procedures.</p>	No impact on safety of the vessel as the event is contained within the ROC.
Vessel is under pilotage	Pilot is on board the vessel. No impact on safety of the vessel as the event is contained within the ROC.	<p>Potential impact on safety if ROC loses control of the vessel. Fallback state(s) shall be agreed by all relevant stakeholders, this can include transfer of control procedures, verification & validation activities.</p> <p>Pilots would need to know fallback procedures prior to pilotage taking place. Communication pathways, roles & responsibilities & potential delays in alternative communication technologies.</p>	No impact on safety of the vessel as event is contained within ROC. Autonomous pilotage needs to be defined & whether instructions from pilot are passed through ROC or direct to vessels on board systems.

Table 6-3: Fire in a Land Based ROC

Analysis.

The analysis identified several hazards, with fire incidents in a land-based ROC. It is assumed that the remote operators will follow company and legal procedures to ensure the safety of personnel when responding to a fire alarm.

Where vessel functions are remotely controlled from the ROC, an evacuation that results in the loss of control of the functions could rapidly escalate into an emergency condition if not adequately considered within the LPM.

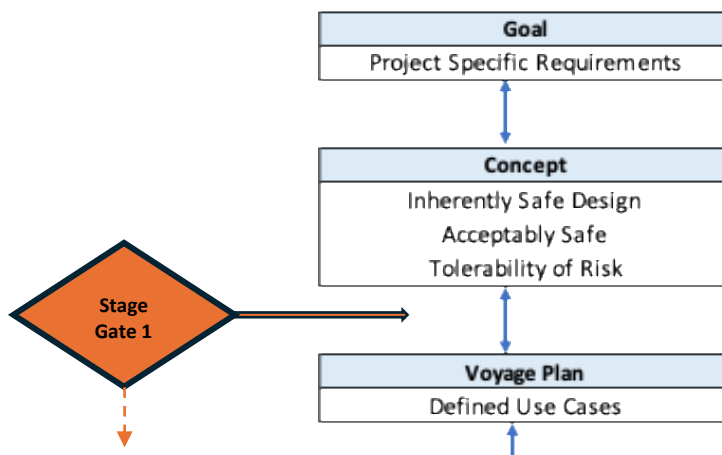


Figure 6-14: Emergency Condition -Fire within a land-based ROC – concept phase review

Plus, additional stage gate reviews can be applied as required, for example, stage gate 2 should identify if the fall-back states align with the layers of protection defined for the MAI.

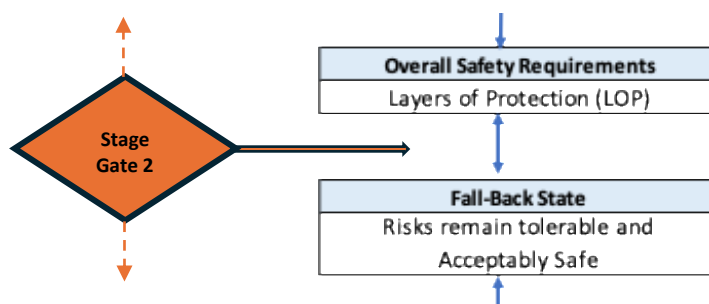


Figure 6-15: Emergency Condition -Fire within a land-based ROC - LoP

Unlike a crewed vessel, where fire alarms are managed directly by the STCW personnel on board, a fire at a land-based ROC would typically rely on external emergency services such as the fire brigade, to

respond to the incident. This reliance may introduce delays in re-entry to the ROC and in restoration of operational control.

The application of multiple stage gates identified several potential constraints, examples of which are:

- **Stage Gate 1** – Tolerability of Risk – When the ROC operator is controlling the vessel functions and there is a requirement to abandon the ROC, the assessment may include the transfer of control to another remote operator, to ensure the vessel remains under control. Potential risk: The transfer of control cannot be verified, and the relevant stakeholders may consider a crewless vessel '*making way*' and '*NUC*' as an intolerable risk. Potential risk mitigation: Train ROC operators to deal with a fire situation, change company procedures to allow trained staff to fight the fires, support this with regular training etc
- **Stage Gate 2** – Fallback state – This state should ensure the risks remain tolerable under reasonably foreseeable abnormal and emergency events. Where transfer of control to another remote operator is required, the design must account for the following factors:
 - Evacuation time from the ROC,
 - Time required to transfer control, and
 - Verification processes to confirm a successful handover.

A failure to regain control within an acceptable timeframe could result in a vessel '*making way*' also becoming a '*vessel not under command*' (NUC) as defined by COLREGS Rule 3, meaning it is unable to manoeuvre and unable to keep out of the way of other vessels. In such circumstances, compliance with COLREGS RULE 72 is essential to ensure the correct navigation lights and day shapes are displayed. This would require the vessel to possess situational awareness to autonomously determine which lights to display if control between the vessel and the ROC is lost.

The overall safety requirements may include a layer of protection to automatically transfer control to the autonomous functions onboard the vessel, or to a qualified operator at another location. This duplication of the remote operator and associated level of resilience must be evaluated for each individual project based on the requirements of the various stakeholders. Furthermore, the evaluation must be re-assessed should there be a change in connectivity providers or ROC personnel.

The transfer of control between ROC's must incorporate verification of software revisions and diagnostic checks to ensure there are no inadvertent changes occurring upon transfer to the new ROC. A formalised and auditable process must be established to verify the successful transfer of control to ensure there is only one station in control at any one point in time.

In addition, if the vessel has embarked personnel, such as crew, service personnel, surveyors, port state control, dock workers etc.), a transfer of control must be immediately communicated to all relevant stakeholders to allow them to make informed decisions regarding safety. For example: a service engineer on board the vessel in coordination with a remote operator to control a function, such as remotely starting or stopping a pump, must be notified that the remote operator is no longer in the control loop. This ensures that the risks to personnel, the ship or the environment do not become intolerable. Additionally, in such scenarios, an agreed fallback state, must be clearly defined and understood by all relevant stakeholders, and implemented as required.

These considerations highlight the necessity of integrating fall-back control strategies allowing the relevant stakeholders to ensure the risk does not exceed the agreed tolerability of risk defined for the MAI.

6.1.4 Use Case 4: Loss of Situational Awareness.

For this use case, I have used the definition of ‘situational awareness’ from Endsley [122],

‘Situation awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future.’

When a vessel function operates under remote control with no crew on board, the remote operator’s situational awareness maybe compromised due to factors, such as:

- the degradation or loss of verifiable data available to the remote operator. Example: camera image degradation due to salt contamination on the lens.
- a technical failure – example: loss of connectivity
- connectivity latency – unable to see up to date information.
- a malicious attack intended to cause harm (e.g. Cyber Attack).
- complacency and automation bias, a phenomenon, that describe a conscious or unconscious response of the human operator induced by over-trust in the proper function of an automated system. R Parasuraman and D Manzey [123].

The loss of situational awareness does not mean the risks become intolerable as the consequences of the loss are to be derived and are use case dependent. For example: if connectivity is used solely for monitoring purposes, a loss of connectivity would not result in an intolerable risk if the vessel function(s) were operating autonomously or manually. However, if the vessel functions are under remote control, a loss of connectivity during critical stages of the voyage, such as those requiring speed or course adjustments could lead to significant and potentially intolerable risks if the remote operator is unable to respond appropriately when required.

In the context of remote-control vessel functions, an intolerable risk arises when the loss of situational awareness leads to scenarios that surpass the capacity for safe intervention that prevent collisions, groundings or violations of COLREGS.

Table 6-4 Loss of Situational Awareness (SA)			
Scenario	Crewed Vessel	Remotely Controlled Function – Crewless vessel	Autonomous Function - Crewless
Normal operation	Situational awareness (SA) is maintained through the integration of the onboard SQEP crew, supported by navigational aids and engineering support technologies designed to enhance operational understanding and decision-making capabilities.	Situational awareness relies on verifiable data being made available to the remote operator and the ability of the operator to understand the information being provided.	Situational awareness will be provided by the on-board technologies that satisfy the principles of an inherently safe design.
Loss of SA	A loss of situational awareness could result in an intolerable risk. Example: An over the air software update that fails or is corrupted, could result in incorrect information being presented to the end user. This could result in human injury, damage (including disruptions) to property, damage to the environment, or economic loss if the end user relies on the information provided.	On a crewless remotely controlled vessel, a loss of situational awareness could result in a collision or grounding event which could have significant safety implications, such as collision, grounding loss of life or damage to the environment. If the loss of SA is due to a loss of connectivity, the ROC operator would be unable to have meaningful control of the vessel functions until connectivity is restored. ROC operator would need to know they have lost SA allowing them to advise relevant stakeholders and take appropriate action, which may include transfer of control to another ROC operator or other entity agreed by the relevant regulatory authorities.	Degradation or failure of SA will be considered during design and where required relevant stakeholders will be advised. The required layers of protection and where required fallback state would need to be derived based on several factors and agreed by the relevant stakeholders

Table 6-4: Loss of Situational Awareness (SA)

Analysis.

The analysis identified several hazards associated with the loss of situational awareness, spanning from minimal or no immediate risk to an intolerable risk that can escalate to an emergency condition within a short time frame (Use Case Dependent). The severity of these risks is influenced by various factors, such as:

- the phase within the voyage plan
- the duration required to regain connectivity,
- the time needed to re-establish meaningful control,
- the duration required to regain situational awareness,
- the time to respond to the new environment.
- the ability of the remote operator to regain situational awareness.

Note that time is an important consideration in dealing with adverse events, and it needs to be explicitly considered in assessing risks when applying the LPM.

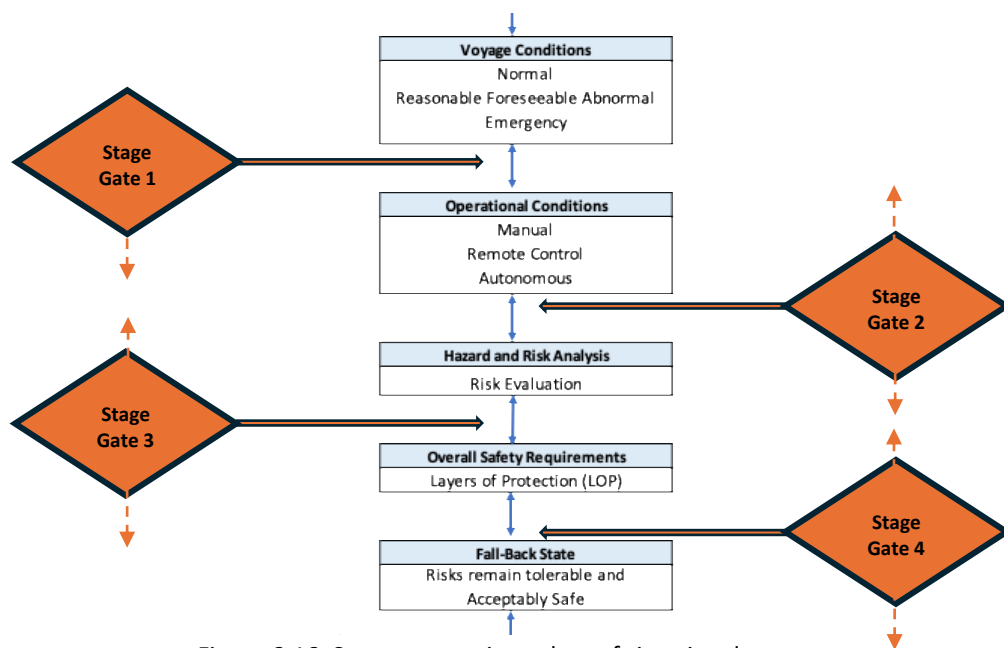


Figure 6-16: Stage gate review – loss of situational awareness

The application of multiple stage gates identified several potential constraints, examples of which are:

- **Stage Gate 1** – During the initial concept development stage of the LPM, the potential loss of situational awareness (SA) must be recognised as a RFAE. Early identification is essential to ensure that the associated hazards, particularly those arising from degraded perception, decision-making, or response capability, are explicitly addressed. Failure to consider this scenario at the outset could result in the emergence of intolerable risks later in the system lifecycle, especially for configurations involving autonomous or remotely controlled operations. Accordingly, Stage Gate 1 serves as a critical checkpoint to verify that such abnormal conditions are systematically integrated into the early hazard identification and risk assessment processes
- **Stage Gate 2** – Operational conditions – The loss of situational awareness should be considered in all three operational conditions (Manual, Remotely Controlled, Autonomous). The treatment of a loss of SA for remote control or autonomous functions on a crewless vessel would need to be considered within Stage Gates 3 and 4 to ensure adequate layers of protection are provided to prevent the risks escalating to an emergency situation.
- **Stage Gate 3** – The tolerability of risk is dynamic and use case dependent, for example: a failure to regain SA where there is no maritime traffic, no danger of grounding and a steady high pressure weather forecast, could provide a greater time for recovery compared to a vessel in a high traffic area, near the coastline and a deteriorating weather forecast. In the latter scenario, if the loss of SA is not swiftly rectified it could escalate to an emergency condition, especially if the vessel is making way.
- **Stage Gate 4** – The application of the layers of protection is again Use Case dependent and would need to be evaluated on a wide range of inputs. If the data are not available, or verifiable, the methodologies used to ensure the risks do not become intolerable must be known and agreed with all relevant stakeholders.

6.1.5 Key findings from the use cases.

The application of the LPM to the selected use cases highlighted several risks that, if not proactively addressed during design and operational phases of the MAI, could rapidly escalate to an intolerable risk.

Use Cases 1, and 2 demonstrated that, on a crewed vessel, demonstration of compliance with COLREGS is effectively managed by the STCW-trained crew. However, the analysis revealed that even relatively simple operational tasks, such as ensuring the navigation lights comply with the regulatory requirements, present substantial challenges when relying solely on current technologies. While keeping the navigation lights permanently on, maybe a possible mitigation, this approach fails to accommodate dynamic operational conditions, potentially leading to regulatory non-compliance.

The complexity of anchoring operations introduces additional challenges that may be difficult to resolve using current technologies and operating procedures. As a complex systems problem, anchoring requires precise execution under diverse environmental and regulatory requirements. Industry feedback highlights reluctance to engage with uncrewed vessel operations, reflecting broader concerns about the ability to recover an anchor when required. Notably, when personally contacted by phone, two leading anchor handling companies expressed reluctance to be included in the approved suppliers list if the vessels were operating with no crew on board for three specific reasons, firstly, the complexity in automating all aspects of the anchoring process, secondly the risk associated with being unable to recover the anchor when required and thirdly the costs associated with the design and maintenance of the equipment. Where 'station keeping' is required by the relevant stakeholders, the application of dynamic positioning technologies maybe a suitable mitigation, if an anchor is not fitted. However, this introduces additional layers of complexity, which in certain cases, could elevate the risks to an intolerable level for some ship owners/operators.

Use Case 3, examined the operational challenges associated with a reasonably foreseeable abnormal event, specifically the activation of a fire alarm within the ROC. In such an event, regulatory and safety protocols may necessitate a prolonged evacuation, significantly delaying the ability of remote operators to re-establish control over the vessel functions. Given that re-entry procedures would

often be dictated by stringent legal and occupational safety requirements, the time to regain meaningful control of an uncrewed vessel could result in the risks becoming intolerable.

Use Case 4, focused on the implications of a loss of SA in both remotely controlled and autonomous operations. The analysis indicates that irrespective of the ‘Operational Condition’ of the vessel, a loss of SA require similar risk mitigation measures to be applied, which includes multiple layers of protection. While a crewed vessel benefits from human oversight, empirical evidence from historical maritime incidents such as the Costa Concordia event that took place in Giglio in 2012 [124] the Ever Given that blocked the Suez Canal in 2021 [125] and the collision of the MV Solong and the Stena Immaculate off the coast of East Yorkshire in 2025 [126] demonstrates that such failures have contributed to collisions, environmental damage and in some cases, an unfortunately loss of life.

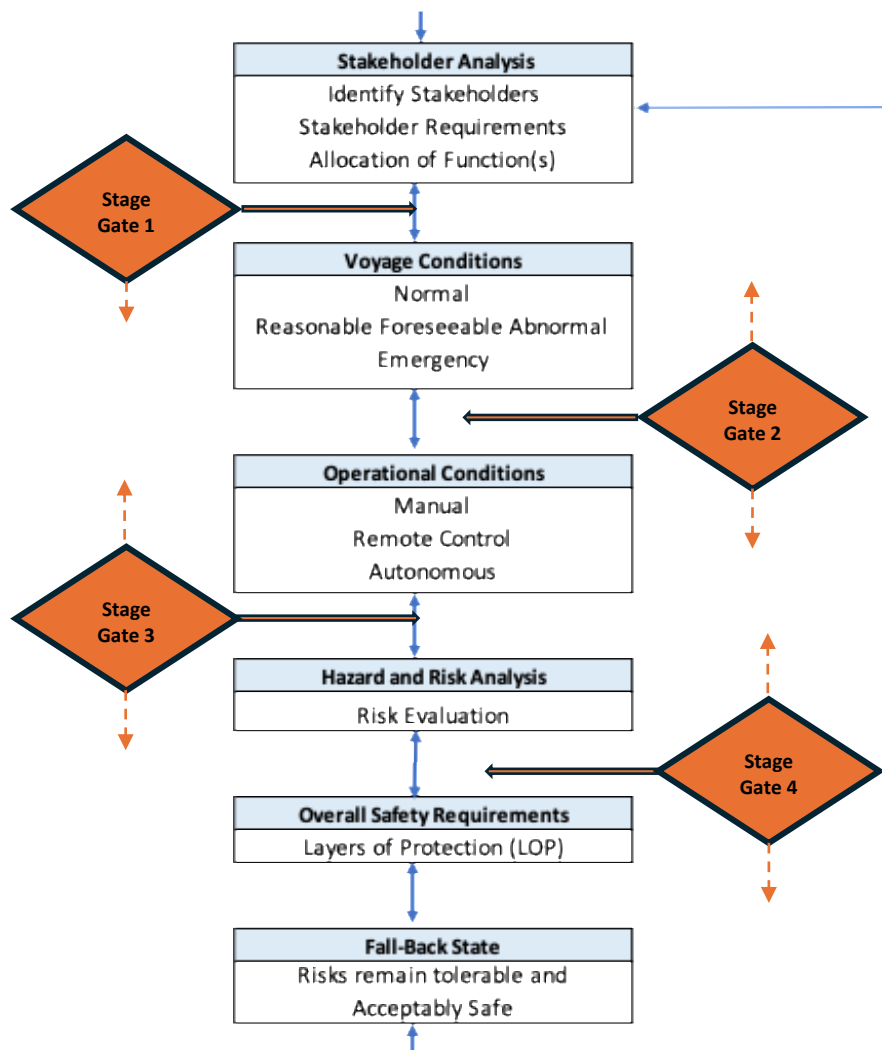


Figure 6-17: Anchoring Stage Gate review

The application of multiple stage gates identified several potential constraints, as follows:

Stage Gate 1 – Stakeholder Requirements - The port authorities can require the vessel to anchor due to congestion in the port, weather conditions etc. They cannot guarantee immediate berthing.

- **Potential risk:** facilities would need to be provided to keep the vessel in position for an undefined period.
- **Potential risk mitigation:** changing ports could be an option, but would that have an impact on the company's original goal?

Stage Gate 2 – Voyage Conditions – The owners have been advised that they cannot guarantee 100% recovery of the anchor. They have also been advised that connectivity to the port location cannot be guaranteed with the current design options being proposed. This could have an impact on safety, the maritime environment or damage to the national infrastructure if the anchor cannot be recovered.

- **Potential risk:** significant environmental damage or risk to submerged infrastructures e.g. data cables, pipelines.
- **Potential risk mitigation:** ensure 100% connectivity is available through multiple connectivity providers. Do not fit anchors (inherently safe design).

Stage Gate 3 – Operational Conditions – The owners wish to operate the vessel in autonomous mode for the duration of the voyage. Port authority and flag-state will not allow this mode when entering the territorial seas or port area.

- **Potential risk:** qualified personnel are unavailable to control the vessel functions remotely, or transfer of control is unachievable due to a technical issue.
- **Potential risk mitigation:** ensure that qualified staff are available and on standby to take remote control of the vessel functions and verify that fall-back states and the layers of protection satisfy the requirements of the relevant stakeholders. Additionally, establish contingency procedures in case vessel is refused entry.

Stage Gate 4 – Overall Safety Requirements – The availability of external assistance within a defined time is only available at 4 of the 5 ports within the voyage. An event that requires external assistance could escalate into an emergency condition with a potential impact on the environment or infrastructure of the port or at a wider national level.

- **Potential risk:** significant financial implications if the event escalates to an emergency condition.
- **Potential risk mitigations:**
 - do not proceed to the port, or ensure external assistance is available.
 - redesigning the anchoring system to support autonomous or remote-control operations.
 - develop fallback states to address a wide range of failure scenarios, such as the availability of external assistance to prevent the vessel drifting due to wind or current.
 - provide means to isolating autonomous functions and collision avoidance systems to allow safe external assistance to be provided, this is an important point as the collision avoidance system would try and prevent a collision occurring.
 - incorporating alternative measures to allow the vessel to hold position, such as a Dynamic Positioning (DP) system.

The analysis of Use Case 2 demonstrates that anchoring operations, particularly under reasonably foreseeable abnormal event or emergency conditions, present significant technical and regulatory challenges when onboard crew are removed. The findings highlight that several key functions, such as the release of sea fastenings, monitoring anchor status, or executing emergency disconnection are currently reliant on human judgement and intervention. In transitioning to remote or autonomous control, these operations require a fundamental redesign supported by validated fallback strategies, and verifiable communication pathways. This use case illustrates the importance of considering an inherently safe design, e.g. using DP systems, as managing risks is unlikely to be practicable with remote or autonomous operations.

The application of the LPM, SPM, MAI-DE, LoP and the stage-gate review structure provides a systematic means to identify and mitigate these risks early in the design phase. Critically, it enables stakeholders to evaluate whether anchoring functionality, as currently designed, can meet

6.1.6 Effectiveness and Gaps in the Lifecycle Process Model.

This chapter has demonstrated the practical application of the LPM in systematically identifying, assessing, and addressing the risks associated with both crewed and crewless maritime operations within the MAI. Through the application of the LPM across the selected use cases, ranging from basic vessel functions such as navigation light operation and anchoring to more complex scenarios such as the abandonment of a Remote Operations Centre (ROC) and the loss of situational awareness (SA), this chapter has illustrated how the LPM promotes structured decision-making, supports safety assurance, and enables the development of a compelling assurance/safety case to demonstrate 'Acceptably Safe' operations in the context of the MAI.

6.1.6.1 Effectiveness of the LPM in Identifying Risks.

The structured and iterative approach of the LPM, ensures that risks are not considered in isolation but rather contextualised within the operational and regulatory framework of the vessel's lifecycle. This process has proven effective in:

- Identifying dynamic and emergent risks that arise from removing onboard crew and relying on remote or autonomous control. For example, the anchoring use case (Section 6.1.2) revealed that even routine operations become complex system-of-systems challenges when the human element is removed, requiring the redesign of fallback states and layered protection strategies.
- Recognising the critical role of reasonably foreseeable abnormal events (RFAEs) in driving fallback state requirements. The analysis of ROC abandonment due to a fire (Section 6.1.3) and the loss of situational awareness (Section 6.1.4) underscores the need to ensure fallback states are not only defined but also robust and validated under realistic abnormal and emergency conditions.
- Supporting cross-stakeholder engagement by explicitly integrating evolving stakeholder requirements and demonstrating the importance of collaborative decision-making in defining tolerable risk boundaries and acceptable fallback solutions, an aspect that would be overlooked in purely technological assessments.

Importantly, this structured lifecycle approach, considering normal, reasonably foreseeable abnormal, and emergency conditions could not have been achieved through more traditional, ad-hoc risk assessments. The LPM's systematic nature ensures that each lifecycle stage builds upon previous assessments and informs subsequent risk management strategies.

Despite its structured framework, the application of the LPM within this chapter also reveals several critical gaps that must be addressed to fully assure 'Acceptably Safe' operations for crewless and autonomous vessels:

6.1.6.2 Residual reliance on human intervention:

While the LPM identifies fallback states and potential automated reversion strategies, key operational functions, such as anchor recovery, navigation light verification, and emergency disconnection of the anchor, remain reliant on human judgement and decision-making. These gaps suggest that current technological maturity and design solutions are not yet fully aligned with the inherently safe design principles outlined in the LPM and SPM.

6.1.6.3 Incomplete validation and verification of fallback states:

While the fallback states are conceptually defined in the LPM, the case studies indicate that these would need to be comprehensively validated under real-world operational conditions, particularly during degraded or emergency scenarios. Without such real-world validation the credibility of fallback states as effective layers of protection (LoP) within the overall safety argument is diminished.

6.1.6.4 Connectivity and communication vulnerabilities:

The analysis highlights that connectivity between the ROC and the vessel constitutes a single point of failure in remotely controlled operations, which could potentially escalate to an intolerable risk. While the LPM identifies these dependencies, it does not prescribe explicit design solutions to ensure communication resilience. Notably, the selection of appropriate design solutions would depend on the configuration and operational context of the MAI, as determined by the relevant stakeholders.

6.1.6.5 Dynamic regulatory harmonisation challenges:

While the LPM acknowledges evolving regulatory and port authority requirements as operational conditions change, there is no clearly defined process within the current LPM structure for resolving conflicts between ROC operators, port authorities, and other regulatory stakeholders in real-time. This absence of a harmonised framework poses a risk to maintaining a unified claim of regulatory compliance during dynamic voyage conditions.

6.1.6.6 Unclear ownership of evidence production for regulatory review:

The chapter does not define who is responsible for producing, validating, and submitting the assurance evidence to satisfy the requirements of the relevant regulatory authorities. This absence of clarity could undermine the credibility and eventual acceptance of the assurance case for uncrewed or autonomous vessel operations and would need to be addressed by the relevant stakeholder.

6.1.7 Evaluation of the research objectives.

This section evaluates the application of the LPM, SPM, MAI-DE and LoP within the use case demonstration, using a series of research questions derived from the thesis aims. The evaluation assesses how effectively the LPM supports risk identification, assurance development, and system understanding in the context of the Maritime Autonomous Infrastructure (MAI).

- **Do the models function effectively when applied to representative MAI use cases?**
Yes. The models have demonstrated its ability to systematically identify, structure, and contextualise risks across multiple operational scenarios, encompassing normal, operations, reasonably foreseeable abnormal events (RFAEs) and emergency conditions. Its lifecycle-based structure enabled traceable analysis from early concept through to operational fallback, supporting robust understanding of risk propagation in distributed, uncrewed systems.

- **Could the same risks have been identified using conventional methods?**

Unlikely. The structured, iterative nature of the MAI revealed emergent and system-level risks that would not typically be exposed through fragmented or static risk assessments. For example, cross-domain interdependencies, such as those between communication networks and fallback states, were identified only through the process-driven flow embedded in the LPM

- **Has the LPM identified new risks specific to crewless operations?**

Yes. The application of the models exposed novel risks associated with the removal of onboard crew, including changes in escalation dynamics, reliance on external actors (e.g., remote operators or reliance on emergency services), and the need to redefine fallback strategies. These risks are not typically addressed in traditional maritime risk models.

- **Do the Models differentiate between the risks of remote and autonomous operations?**

Yes. The models were able to distinguish operationally specific risk characteristics. Remote operations were shown to be more susceptible to human situational awareness degradation and connectivity disruptions, whereas autonomous operations presented unique challenges in fallback validation and technology sufficiency

- **Is the integration of the SPM and LoP models essential to the LPM's effectiveness?**

Yes. The Safety Process Model (SPM) and the Layers of Protection (LoP) model are critical to validating that the risk controls identified through the LPM are not only conceptually robust but also independently verifiable. These elements enable justification that fallback strategies and layered defences collectively support a credible and defensible claim of 'Acceptably Safe'.

- **What gaps remain in the current implementation?**

One significant gap is the absence of an explicit mechanism for defining evidence ownership and responsibility for producing and maintaining the assurance case. This is particularly problematic in a system-of-systems context, where safety evidence is distributed across technical, organisational, and legal boundaries. Without clarity in who is accountable for producing, maintaining, and submitting assurance evidence, stakeholder confidence and regulatory acceptance may be compromised.

6.1.7.1 Final Reflections

In summary, the application of the LPM, SPM, MAI-DE and LoP models within this thesis demonstrate their utility as a structured and context-aware framework for risk identification, assurance development, and system integration within the MAI. The framework proved effective in uncovering emergent risks, clarifying operational responsibilities, and supporting traceable, lifecycle-aligned assurance arguments across different configurations of crewless operation.

However, the evaluation also identified several areas that require further development to ensure regulatory and stakeholder confidence. These include: the validation of fallback states under degraded conditions; resilience of the communication architecture; assurance of autonomous decision sufficiency; dynamic regulatory harmonisation across jurisdictions; and the assignment of evidence ownership within a multi-actor system.

These findings reinforce the core argument of the thesis: that the safe deployment of the Maritime Autonomous Infrastructure is not merely a function of technical performance, but a complex, socio-technical systems problem requiring rigorous lifecycle-based assurance processes, stakeholder-informed fallback states, and robust evidence of safety within a SoS assurance framework. The LPM and its supporting models offer a defensible pathway toward achieving this, but real-world implementation will depend on further development of institutional capability and regulatory alignment across all relevant stakeholders.

The next chapter contextualises these findings within the broader regulatory, operational, and institutional landscape, examining the barriers and challenges to adoption, the limitations of existing governance frameworks, and the enabling conditions under which the MAI may be credibly recognised as meeting the requirement of 'Acceptably Safe'.

Chapter 7 : Barriers and Challenges.

While this thesis establishes a structured framework for the safe development and assurance of the Maritime Autonomous Infrastructure (MAI), the transition from technical feasibility to regulatory and stakeholder acceptance remains uncertain. This chapter analyses the systemic, regulatory, institutional, and cultural barriers that must be overcome for the MAI to become acceptable across jurisdictions.

The central argument is that barriers to acceptance are not caused solely by unresolved technical issues, but also by institutional inertia that is constrained by entrenched practices, fragmented regulatory jurisdictions, lack of clarity around roles and responsibilities, and an underdeveloped understanding of the systemic nature of the MAI as a cross-sectoral, socio-technical infrastructure. Without proactively addressing these barriers, even the most robust compelling technical body of evidence required to justify the claim of 'Acceptably Safe' may fail to gain traction with those ultimately responsible for certification.

One of the most significant challenges facing the acceptance of the MAI is the widespread lack of understanding of what it comprises. The term 'infrastructure' is often misinterpreted as referring solely to shipboard technologies, when the MAI encompasses a complex socio-technical system that spans multiple domains, land, maritime, and space. It includes not only the vessel but also the ROC, connectivity providers, satellite services, external assistance frameworks, and the regulatory and assurance ecosystem that supports these functions.

This misunderstanding perpetuates a vessel-centric model, in which safety is conceived as a static property assessed at the point of design or construction. In contrast, the MAI demands a lifecycle assurance model, as introduced in this thesis through the LPM. Such a model accommodates changing operational modes, evolving stakeholder community roles, and varying jurisdictional requirements, sometimes within a single voyage. This dynamic infrastructure needs to be understood by the regulators and stakeholders to evaluate the MAI effectively.

The regulatory framework surrounding the MAI currently remains fragmented, with differing requirements emanating from individual stakeholders. Unlike traditional vessels that are subject to flag and port state control under established conventions (e.g. SOLAS, STCW, COLREGS), the MAI introduces cross jurisdictional ambiguities and local requirements that can differ between jurisdictions. These ambiguities create uncertainty about which authority holds ultimate accountability for safety assurance, particularly during dynamic events such as control transfer, degraded function, or connectivity loss.

Further uncertainties could exist relating to how the regulators and relevant stakeholders would interact with the ISA. Some of the questions that remain unresolved are:

- Who commissions and pays for the ISAP to be carried out – how do we avoid a conflict of interest?
- Whether ISA findings are binding?
- What happens if the ISA and the flag-state disagree?

In practice, liability is likely to rest with the vessel operator or owner, regardless of third-party assessments. However, in the absence of clear legal precedent, insurers may refuse to underwrite operations even if the assurance/safety case is technically robust. This lack of clarity regarding ultimate responsibility and stakeholder endorsement can create significant challenges in achieving regulatory approval or acceptance, as the assurance/safety case must often be recognised and endorsed by all relevant stakeholders to be considered credible and enforceable.

Another challenge is the ambiguity over who is responsible for generating the compelling body of evidence to demonstrate the MAI is 'Acceptably Safe' to operate in a defined context of use. In conventional vessel certification, this responsibility lies with the shipbuilder and is verified by the classification societies. For the MAI, where functionality is shared across multiple stakeholders, including ROC designers, software providers, and network operators, accountability can become diluted. Without a clear process in the development of the assurance/safety case, which this thesis aimed to address, it may lack both credibility and regulatory acceptance.

While this thesis does not explicitly address the business case for autonomy, it acknowledges that developing and maintaining a dynamic assurance/safety case across multiple jurisdictions, and fallback scenarios may be seen as prohibitively complex or costly, further impeding its adoption.

The acceptance of the MAI is fundamentally a question of alignment across sectors, regulators, functions, and stakeholders. As demonstrated within this thesis, even the most robust technical design will struggle to achieve operational approval without systemic changes to how maritime assurance/safety is conceived, managed, and assured.

The challenges discussed within this thesis reflect a broader problem: *'the current maritime system is not structured to govern infrastructures that extend beyond the vessel itself'*. Therefore, the MAI must not be treated as a product or platform, but as a capability-enabling SoS infrastructure, requiring new models of governance, assurance, and stakeholder engagement.

7.1 Transitioning from static to dynamic assurance models for the MAI

This thesis establishes that the constituent elements of, and relevant stakeholders for, MAI can be identified, thereby forming a conceptual model of a 'Global MAI'. The assurance/safety case that underpins the compelling body of evidence submitted to regulatory authorities for regulatory approval is constructed with reference to this system wide configuration.

Unlike conventional vessels which operate within a relatively static assurance environment, the MAI is a dynamic, distributed, and reconfigurable system-of-systems. Accordingly, this thesis asserts that a static one-size-fits-all assurance/safety case is inadequate. Instead, the assurance/safety case, must be developed for each planned voyage, tailored to the specific configuration of the MAI elements. These include the vessel, port infrastructure, ROCs, communication networks, emergency response arrangements, supporting services, operational dependencies, along with stakeholder obligations, each potentially characterised by varying levels of maturity, capability, and risk exposure.

Each MAI element must be supported by an individual assurance/safety case that defines its functional capabilities, operational limitations, and dependencies on other MAI elements. These individual assurance/safety cases must then be integrated into a voyage specific assurance/safety case, which forms the pinnacle/focal point for demonstrating that the configured MAI satisfies both requirements for 'seaworthy' [67] [127] [128] and those of 'Acceptably Safe'.

The adoption of this methodology represents a fundamental shift for the maritime sector. Traditional safety assurance practices, including those defined by classification societies, have historically focused on the vessel as the primary unit of analysis. In contrast, the MAI requires a multi-layered assurance/safety case that spans multiple system domains, organisational structures, and jurisdictional boundaries.

Moreover, the per-voyage assurance case must be aligned with the operator's Safety Management System (SMS), defining how they intend to operate the MAI based on the capabilities and constraints of the MAI elements. This alignment ensures that the SMS dynamically reflects changes in the configuration or performance of MAI elements, as required by the LPM [Figure 5-1]. For example, transitions between operational conditions (manual, remotely controlled, or autonomous), which have not been evaluated through the application of the LPM, SPM, MAI-DE and LoP, or changes in environmental conditions that exceed the requirements associated with the operational concept, may invalidate previously accepted safety assumptions. In such cases, the assurance/safety case must be re-evaluated.

The implications of this approach are significant for both regulatory authorities and other relevant stakeholders such as insurers. From a regulatory perspective, this model challenges legacy assumptions of static certification and demands new frameworks for dynamic and context-sensitive evaluation as defined within this thesis. From an insurance perspective, the per-voyage assurance case could serve as a critical input for underwriting, offering a structured and auditable demonstration of risk management. In line with the Marine Insurance Act the per-voyage assurance/safety case supports the obligation of the shipowner to provide a *"fair presentation"* by *"disclosing to the insurers of every material circumstance which the insured knows or ought to know, and one that ensures that every material representation as to a matter of fact is substantially correct and every material representation as to expectation or belief is made in good faith. including dependencies on external systems and fallback provisions."*

In summary, this thesis advocates a fundamental reconfiguration of safety assurance in the maritime sector. The per-voyage assurance/safety case methodology is both a practical and conceptual response to the complexities of the MAI and represents a necessary evolution in regulatory thinking, stakeholder responsibility and system assurance. While implementation may require broader

structural and legal reform, potentially beyond the current remit of international regulatory bodies such as the IMO, this shift is essential for enabling demonstrably safe and insurable autonomous maritime operations

The barriers outlined in table 7-1 are highly interdependent and reflect the systemic complexity inherent to the MAI. At the foundational level, the absence of a single approval authority and the lack of clarity around the constituent elements of the MAI impedes effective stakeholder coordination. This challenge is further compounded by a fragmented regulatory landscape, that extend beyond the traditional maritime domain. This fragmentation necessitates not only comprehensive stakeholder mapping but also cross-sectoral collaboration to ensure regulatory coherence.

Procurement and contractual arrangements provide further challenges, where traditional models based on fixed responsibilities must evolve toward shared accountability to reflect the distributed nature of system-of-systems (SoS) operations.

Additionally, the failure to recognise that the assurance/safety case must be maintained dynamically, throughout the lifecycle of the MAI. This requirement becomes increasingly complex when the MAI spans multiple jurisdictions or undergoes reconfiguration during a single voyage.

Compounding these issues is a lack of established competency frameworks for any of the actors, tailored to SoS environments and over-reliance on legacy maritime practices, limiting the sector's ability to draw on proven assurance methodologies from more advanced domains such as aerospace and nuclear.

This misalignment becomes particularly problematic when divergent views between Independent Safety Assessors (ISAs) and regulators emerge. Such conflicts raise unresolved questions about liability, insurability and the validity of the assurance/safety case itself.

Ultimately, these barriers are mutually reinforcing making it essential to adopt an integrated, adaptive approach to achieve a coherent and credible safety assurance framework, and one that aligns with the dynamic, cross jurisdictional nature of the MAI. The LPM developed within this thesis offers a

structured pathway to achieve this, supporting a credible and context sensitive assurance framework across all operational conditions.

This approach highlights a fundamental distinction between the MAI and conventional maritime systems. Whereas legacy approval and acceptance processes assume static certification based on a set of prescriptive requirements, the MAI requires a dynamic, per-voyage assurance model that considers all elements to ensure the claim of 'Acceptably Safe' is demonstrably achieved. This distinction represents one of the unique contributions of this thesis: the reframing of maritime assurance/safety cases as a dynamic and system-of-systems problem, rather than a vessel-centric certification exercise.

Barriers and Challenges	Mitigation
The elements that form the MAI are not identified and that no single approval authority exists for the MAI.	Stakeholder mapping will be required for all operational conditions of the MAI.
The traditional approach to vessel procurement needs to change	Contracts developed with shared responsibilities
Not recognising that multiple regulatory requirements exist	This will require collaboration with the relevant stakeholders
Failure to understand that the assurance/safety case must be maintained throughout the life of the MAI	Skilled personnel able to develop and maintain the assurance/safety case will be required
Competency requirements to work within a SoS environment does not exist within a company	Ensure required skills are available through external sources.
Reliance on sectors outside of maritime domain to demonstrate 'Acceptably Safe' & willingness to adopt and tailor existing good practices and not rely on existing processes or develop new ones	Increase competence of all sectors engaged with the MAI, not just Maritime
Dynamic nature of assurance/safety case, stakeholder community & regulatory requirements possibly within single voyage, is not understood.	This risk could result in vessel being detained or refused entry into port. Use of LPM, SPM, MAI-DE and LoP is recommended.
What happens if the ISA says no, but the regulator says yes, are implications understood?	Realistically, it is the owner's risk, no matter what the ISA recommends, but how would the insurers react?

Table 7-1: Barriers - Challenges and Mitigations in acceptance of the MAI

Chapter 8 : Evaluation, Future Work and Conclusions.

8.1 Independent Evaluation.

The evaluation of this thesis was undertaken by a group of external specialists, selected for their demonstrated expertise, professional experience, and relevance to the subject matter. To preserve impartiality and ensure integrity of the evaluation process, the reviewers were anonymised and are referred to by number only as shown in Table 8.1. The evaluation process was conducted through a combination of structured face-to-face meetings, written correspondence, and online discussions held during May and June 2025.

The individuals consulted for this evaluation brought diverse yet complementary perspectives from academic, regulatory, and industrial backgrounds. While several reviewers hold doctoral-level qualifications, others contributed extensive experience through senior roles in, safety-critical systems engineering, maritime regulatory development, human-centred design and psychology. This multidisciplinary panel provided a credible and contextually informed basis for assessing the applicability, completeness, and rigour of the frameworks developed in this research.

Participant	Date	Qualification	Experience
1	07-Jun-25	PhD	Occupational psychology with extensive maritime experience
2	22-Apr-25	PhD	Safety and security specialist
3	13-Jun-25	PhD	Extensive maritime, systems and safety experience
4	17-Jun-25	PhD	Human Factors specialist and recognised world expert within the maritime sector
5	17-Jun-25	MSc	Renowned maritime expert on regulatory development
6	16-Jun-25	MIET, MSc	Extensive maritime systems assurance experience
7	09-May-25	FIMarEST	Professional engineer with extensive naval and commercial experience
8	10-Jun-25	MEng	Safety specialist with maritime, aerospace, and land-based experience

Table 8-1: Overview of anonymised reviewers and professional backgrounds.

The feedback provided by the external reviewers offered valuable insight into the strengths, limitations, and applicability of the Maritime Autonomous Infrastructure (MAI), Lifecycle Process Model (LPM), Safety Process Model (SPM), Maritime Autonomous Infrastructure- Design Envelope (MAI-DE) and the Layers of Protection Model (LoP) developed in this research. Overall, the evaluation confirmed that the thesis addressed a timely and significant gap in the field of maritime autonomy, namely, the lack of a structured SoS approach that extends beyond the vessel to encompass the wider supporting infrastructure, safety assurance requirements, systems integration, and regulatory adaptability. The following key themes emerged from the external evaluation, the first five are responses to questions posed by the author, but the sixth is an issue that arose from the discussions:

- **Q1: Lifecycle Coverage and Completeness:** Does the model encompass all essential stages of the Maritime Autonomous Infrastructure (MAI) lifecycle? Are there any critical omissions?
 - Reviewers broadly agreed that the LPM addressed the key stages of the MAI lifecycle. However, several highlighted the need to further develop those phases in which responsibility transitions occur, particularly at interfaces between subsystems, stakeholders/actors or regulatory domains. These transitional boundaries were seen as critical points of vulnerability, where assurance/safety continuity must be explicitly maintained.
- **Q2: Conceptual Clarity and Communication:** Is the model clearly structured and effectively communicated? Could any components be refined for improved understanding?
 - While the model's structure was broadly understood, reviewers recommended improvements in explanatory clarity, particularly for audiences without prior experience with systems engineering or safety case methodologies. Enhanced use of consistent terminology and domain relevant examples was advised to support broader comprehension and engagement. In particular, the use of clearer terminology and more illustrative examples was advised to enhance accessibility and understanding.

- **Q3: Alignment with Established Practices:** Does the model align with recognised industry practices and regulatory expectations? Are there any identifiable risks or inefficiencies?
 - The frameworks were regarded as consistent with recognised industry safety practices and regulatory expectations. Nevertheless, reviewers emphasised the importance of validating the model under real-world operational conditions to assess its practical effectiveness, reveal any latent inefficiencies, and ensure that underlying assumptions are substantiated by operational evidence.

- **Q4: Operational Applicability:** Can the model be practically applied to real-world autonomous maritime projects? What challenges might emerge in implementation?
 - Two reviewers advocating for the application of the models in a real-world case study to strengthen their relevance and demonstrate their capacity to support decision-making in complex, operationally dynamic environments. One reviewer reported preliminary use of the models within their organisation, that the model had already been used within their organisation where it was employed to identify risk interfaces, suggesting early evidence of operational relevance.

- **Q5: Enhancement Opportunities:** What specific amendments or additions could enhance the model's utility, rigour, or comprehensiveness?
 - Suggestions for improvement included further articulation of the thesis's unique contributions, clearer differentiation from traditional shipbuilding assurance processes, and the inclusion of additional guidance material for practitioners unfamiliar with autonomous or remotely controlled maritime systems.

- **Intended Audience:** Who is the research in its current form, most accessible or usable by, and what level of education, expertise, or domain specific knowledge would be required to interpret and apply it effectively.?
 - Feedback indicated that the thesis is most accessible to individuals with postgraduate-level education and domain-specific expertise in maritime systems or safety assurance. While reviewers recognised the novelty and rigour of the framework, several emphasised the limited pool of experts currently capable of interpreting and applying the models. To broaden its usability, it was recommended that additional practitioner-oriented material or explanatory tools be developed to support wider engagement.

These findings directly informed a series of revisions to the thesis, including enhanced clarity in the model's structure, improved articulation of the unique contributions to the assurance of the MAI, and refinements to illustrative examples to improve stakeholders/actors understanding, and relevance of the models produced within this thesis. Collectively, the changes have strengthened the academic rigour, and practical applicability of the models within the context of the MAI.

The external evaluation not only highlighted the strengths of the LPM, SPM, MAI-DE, and LoP models, but also identified areas requiring further development, particularly at the interfaces between regulatory domains and during transitions of responsibility. In response, the proposal was updated in several areas. Firstly, the discussion of transitional boundaries was expanded, with greater emphasis placed on the need for explicit assurance continuity at subsystem, stakeholder, and jurisdictional interfaces. Secondly, clearer terminology and more practical examples, making the models accessible to a wider audience, including those without a background in systems and safety engineering. Finally, the importance of continuous validation and adaptation has been emphasised, recognising that regulatory and operational contexts will continue to evolve.

8.2 Future Work: Legal and Regulatory Challenges: The Road Ahead

This section reflects the expanded analysis and feedback presented in Sections 7 and 8.1, ensuring that the conclusions and future work are fully aligned with the latest evaluation and regulatory context.

While this thesis has developed a structured safety assurance framework for the Maritime Autonomous Infrastructure (MAI), three critical areas require further exploration to ensure long-term viability and stakeholder acceptance:

- (1) achieving and adapting to regulatory change,
- (2) integrating business risk and economic viability, and
- (3) embedding human-centred design in all phases of MAI development.

These priorities have been shaped by the insights gained from the independent expert review and the evolving regulatory landscape discussed in the preceding sections.

8.2.1 Regulatory Change as a Dynamic Constraint

The regulatory landscape for the MAI is inherently fluid, reflecting evolving international (e.g., IMO MASS Code) and national legal frameworks. Although this thesis has proposed a flexible assurance approach adaptable across jurisdictions, future work should address how to:

- Dynamically incorporate regulatory changes into the Lifecycle Process Model (LPM) and Safety Process Model (SPM) and, where possible, help to shape that evolution,
- Evaluate the potential for divergence in national implementation of international guidelines, including the impact on fallback states and liability regimes.
- Develop a Regulatory Change Impact Model (RCIM) and associated Regulatory Change Impact Analysis (RCIA) to systematically assess how new or amended regulations influence the assurance/safety case and stakeholder acceptance.
- Define and test procedure for ROC outside of the flag of registry, including reporting chains, authority transfer protocols, and evidential continuity for investigations.

- Systematically incorporate workplace HSE, data protection, cyber security and comms licensing requirements into the SPM (as jurisdictional subclaims) and verify them within the ISA scope.

This work is essential to ensure that safety claims remain valid and defensible as regulatory expectations evolve.

8.2.2 Business Risk and Economic Justification

While outside the primary scope of this thesis, ‘business risk’ represents a critical factor in the acceptance and deployment of the MAI. Economic viability underpins the willingness of stakeholders to invest in crewless or autonomous operations. Future work should explore:

- The lifecycle economic implications of different MAI ownership and operational models, such as partnerships or leasing structures.
- The intersection of economic risk and safety claims, particularly when cost-saving measures (e.g., reduced crewing or fuel use) influence system design and fallback strategies.
- How insurers, financiers, and charterers evaluate the assurance/safety case in the context of evolving market conditions and regulatory obligations, and the potential impact on OPEX from revised insurance premia.
- The development of assurance cases for the ROC and connectivity providers (availability, latency, cyber posture) and evaluate their effect on the OPEX/CAPEX and on the strength of the assurance/safety case.

One potential avenue of research is the development of ‘techno-economic models’ that link safety assurance frameworks to commercial viability, providing decision-makers with holistic evidence for investment and operational decisions.

8.2.3 Human-Centred Design

As vessels transition toward autonomous and remotely controlled operations, human-centred design (HCD), must remain a core principle within the MAI. While onboard crew presence may be reduced or eliminated, human actors, such as remote operators, shore-based maintainers, and even third-party responders, remain critical to the MAI's operation and safety claims. Future research should:

- Examine how HCD principles can be systematically applied within the LPM and SPM to ensure that interfaces, workloads, cognitive demands, and decision-support tools align with human capabilities.
- Investigate the training, certification, and organisational roles required for humans interacting with the MAI across its lifecycle.
- Develop metrics and assurance arguments that account for human performance variability, and integrate these into assurance/safety cases
- Explore how stakeholder trust is influenced by transparency, explainability, and confidence in human-system interactions.
- Investigate recognition of operator competencies and authorisation limits across jurisdictions and specify evidential requirements within the assurance/safety case.

Neglecting the human dimension risks creating serious challenges in demonstrating that the MAI is 'Acceptably Safe'. Recognition and integration of the human as a core system element, regardless of whether the MAI operates autonomously, remains essential to its overall safety assurance.

8.2.4 Intangible assets and the prospect of self-certification of the MAI

As the MAI continues to evolve, future revisions to its formal definition must incorporate intangible assets that exert significant influence on its design, operation, and assurance. These assets encompass non-physical elements such as regulatory expectations, contractual obligations, business model viability, and stakeholder trust, each of which plays a foundational role in determining whether the MAI can be considered 'Acceptably Safe'. Accordingly, the revised definition of the MAI would be:

The ‘Maritime Autonomous Infrastructure (MAI)’ is a comprehensive and multifaceted socio-technical set of elements consisting of physical, digital, tangible and intangible assets that support the safe operation of autonomous or remotely controlled functions of a vessel’

One of the most profound potential shifts arising from the integration of such intangible considerations is the move towards the possibility of ‘**self-certification**’ of the MAI or its constituent elements. In contrast to traditional maritime practice, which relies on third-party classification societies and flag-state authorities to issue compliance certificates, a self-certification model would place greater responsibility on the operator or system developer to generate, maintain, and justify the assurance case. Such a transition, while offering flexibility and responsiveness in fast-evolving technological domains, represents a radical departure from existing norms, and raises critical questions about oversight, liability, and the credibility of safety claims.

For the maritime sector, any movement towards self-certification of MAI elements would only be credible if it was supported by robust frameworks for internal governance, evidence generation, and stakeholder accountability. Many of these requirements are anticipated in the LPM and supporting assurance structures proposed in this research, which can be extended to provide the traceability, transparency, and evidence management required for credible self-certification regimes ensuring that assurance remains robust even as certification responsibilities shift from external authorities to operators or system developers.

Future work should therefore explore the institutional, legal, and technical preconditions under which a self-certification regime might be both feasible and legitimate for the MAI. This includes examining how intangible assets such as legal flexibility, commercial drivers, and public confidence intersect with the assurance case, and how these might be systematically embedded into the definition, design, and validation of the MAI itself.

8.2.5 Legal and Regulatory Challenges for the MAI

Navigating the legal and regulatory landscape for Maritime Autonomous Infrastructure (MAI) presents considerable complexity and remains subject to ongoing evolution. Operations can span multiple jurisdictions, encompassing flag states, port states, and the location of Remote Operations Centres (ROCs). Such cross-border activities introduce challenging and complex questions regarding which authority holds ultimate responsibility for safety, incident investigation, and enforcement, especially when ROCs are located outside the flag state's territory. Persistent uncertainties, such as the **"Genuine Link"** required by UNCLOS and the attribution of legal responsibility in case of incidents have yet to be resolved within current regulatory frameworks.

To address these challenges, the LPM and SPM developed within this thesis, requires explicit stakeholder and actor analysis, ensuring that both statutory and non-statutory stakeholders across all relevant jurisdictions are considered. The models also support the definition and validation of procedures for ROCs outside the flag of registration, including the establishment of reporting chains, authority transfer protocols, and evidential continuity for investigations. By embedding these requirements into the assurance process, the model provides a structured approach to managing jurisdictional complexity and ensuring legal accountability.

Additional challenges include the allocation of liability and responsibility when incidents involve autonomous or remotely operated vessels and in the potential shift from third-party certification to self-certification models. While self-certification could increase flexibility and responsiveness, it raises concerns about oversight, credibility, and legal enforceability. Addressing these issues will require ongoing research into the institutional, legal, and technical preconditions necessary for legitimate self-certification. This includes the development of robust internal governance structures, transparent evidence generation processes, and stakeholder accountability mechanisms to ensure that self-certification regimes are both credible and effective.

Traditional maritime assurance is typically reliant on static, prescriptive compliance assessed at the point of design or construction. In contrast, the MAI requires a dynamic, per-voyage assurance approach capable of adapting to changing operational, regulatory, and stakeholder requirements, even within a single voyage. The LPM is inherently adaptive, supporting per-voyage assurance cases

that integrate the latest regulatory, operational, and stakeholder requirements. This adaptability enables operators to demonstrate compliance and safety in a timely manner, thereby facilitating regulatory approval and operational flexibility.

For example, an autonomous vessel conducting a coastal survey may be required to transition from full autonomy to remotely controlled operation when entering a congested port or restricted area. Under the LPM, such a change in operational condition would trigger a per-voyage validation of the vessel's configuration, including confirmation that fallback functions, communication links, and human-machine interfaces remain viable within the approved MAI-DE. This ensures that the assurance/safety case reflects the current operational context and that all relevant stakeholders, such as flag, port, and operator, retain confidence in the vessel's compliance and the continued tolerability of risk. This adaptability enables the assurance case to remain current, evidence-based, and transparent throughout the voyage, thereby facilitating regulatory acceptance and supporting safe, flexible operations within the MAI.

As the regulatory environment continues to evolve, the adaptability and evidence-based nature of the proposed assurance frameworks will be essential. These considerations set the stage for the broader conclusions and implications of this research, discussed in the following section.

8.2.6 Evaluation of Validity and Adoptability of the Thesis

The validity and adoptability of the proposed frameworks have been assessed through a combination of expert review, industry feedback, and application to representative use cases. External practitioners, including those from GE Marine Engine Service and delegates at the RINA Warship 2025 Conference, provided constructive feedback on the practical relevance and scalability of the LPM, SPM, LoP and MAI-DE, along with their supporting frameworks.

Validation was achieved by applying the framework to real-world scenarios, where its effectiveness in risk identification and mitigation was confirmed. Feedback from industry experts indicated that the frameworks are robust and adaptable to varying operational contexts, enhancing their credibility and practical value.

In terms of adoptability, early feedback from practitioners suggested that the LPM and its supporting frameworks are transferable beyond academic contexts, with successful application reported in manufacturing planning and risk management activities. This feedback was instrumental in refining the structure and clarity of the models, leading to the inclusion of additional explanatory material and practical examples to enhance accessibility for a wider audience. Reviewers feedback led to clearer distinctions from traditional shipbuilding assurance processes and placed greater emphasis on transitional boundaries and responsibility allocation.

While these developments indicate strong potential for practical adoption, the broader regulatory context must also be considered. The adoption of new regulatory principles by the International Maritime Organization (IMO) is historically a protracted process, often characterised by incremental change and a reactive posture following major incidents. The IMO's consensus-driven approach, involving extensive negotiation among member states and industry stakeholders, means that even well-evidenced and urgently needed reforms can take many years to be codified into binding international instruments. As observed with the development of the Maritime Autonomous Surface Ships (MASS) Code, regulatory evolution is typically cautious, with non-mandatory guidelines and experience-building phases preceding any move towards mandatory requirements. Consequently, while the principles embedded within this thesis, such as lifecycle assurance, stakeholder-driven safety cases, and system-of-systems risk management, align with emerging best practice, their formal adoption by the IMO is likely to be a gradual process, potentially spanning a decade or more

In contrast, for vessels operating exclusively within the territorial seas of a nation state and thus outside the direct remit of the IMO, the pathway to adoption may be considerably shorter. National maritime authorities possess the regulatory agility to implement innovative assurance frameworks and adapt to technological advances without the need for international consensus, such as seen with the North Sea MOU [133]

Several countries have already demonstrated a willingness to issue their own requirements for autonomous vessel operations, often drawing on or anticipating international developments but tailoring them to local contexts and risk tolerances. As such, the frameworks and methodologies proposed in this thesis may find more immediate application at the national level, serving as a model for early adopters and potentially influencing the direction of future international regulation.

8.2.7 Conclusions

This thesis set out to develop a structured safety assurance framework for the Maritime Autonomous Infrastructure (MAI), addressing the need for a system-of-systems (SoS) approach that extends beyond the boundaries of the vessel to include the infrastructure, stakeholders, and regulatory requirements.

The research was motivated by a clear gap in existing practices: namely the absence of a coherent methodology for assuring the safety of distributed maritime systems operating autonomously or under remote control. To address these challenges, the unique contribution of this thesis lies in the development of four interlinked frameworks: the Lifecycle Process Model (LPM), the Safety Process Model (SPM), the MAI Design Envelope (MAI-DE), and the Layers of Protection (LoP) model. Collectively, they provide a comprehensive, scalable approach to hazard identification, risk management, assurance argumentation, and context-sensitive validation of safety claims within a system-of-systems context. This enables relevant stakeholders to collaboratively demonstrate that the risks associated with autonomous and remotely operated maritime systems are identified, understood, and managed to a level that meets agreed safety expectations.

Furthermore, the models support the definition and validation of procedures for ROCs operating outside the flag of registration, including the establishment of reporting chains, authority transfer protocols, and evidential continuity for investigations. By embedding these requirements into the assurance process, the models provide a structured and adaptive approach to managing jurisdictional complexity and ensuring legal accountability.

A significant challenge remains in the allocation of liability and responsibility in the event of incidents involving autonomous or remotely operated vessels. The potential transition from third-party certification to self-certification, while promising increased flexibility and responsiveness, raises concerns regarding oversight, credibility, and legal enforceability. Addressing these issues will require future research into the institutional, legal, and technical preconditions necessary for legitimate self-certification, including the development of robust internal governance and stakeholder accountability mechanisms.

While these frameworks have been evaluated by subject matter experts and demonstrated through representative case studies, full-scale validation of the frameworks in diverse operational environments has yet to be conducted, and further work is required to assess its effectiveness under real-world conditions, particularly during transitions of responsibility and in the face of evolving regulatory requirements. Additionally, the current pool of practitioners with the necessary expertise to apply the models is limited, highlighting the need for further practitioner-oriented guidance and training materials. Future research should therefore focus on broader industry trials and the development of supporting resources to facilitate adoption and continuous improvement of the frameworks.

The findings indicate that enabling maritime autonomy or remote control of crewless vessel functions demands not only technological innovation but also a wider cross-sectoral and socio-technical transformation, including adaptation to evolving regulatory, operational, and economic contexts.

The realisation of the MAI will require international collaboration, the development of flexible legal frameworks, and a collective willingness to re-examine and evolve the foundational assumptions of maritime regulation. While legal, economic, and organisational aspects have been acknowledged, they were not modelled in detail within this thesis and warrant further investigation. Accordingly, future research should focus on broader industry trials and the development of supporting resources to facilitate adoption and ensure continuous improvement of the frameworks.

In summary, as the thesis progresses to its conclusion, it reinforces its unique contributions by establishing a structured framework that enables the development of a compelling body of evidence to support the claim that the Maritime Autonomous Infrastructure (MAI) is 'Acceptably Safe' to operate within a defined context of use. By integrating hazard identification, assurance argumentation, and validation strategies across the full operational lifecycle of the MAI, the research provides a scalable and defensible approach to safety assurance within a system-of-systems context. This establishes a basis upon which the relevant stakeholders can collaboratively demonstrate that the risks associated with autonomous and remotely operated maritime systems are identified, understood, and managed to a level that is acceptable to the relevant stakeholders.

Chapter 9 : Bibliography.

- [1] ISO/IEC/IEEE 21839- 2019 – Systems and Software Engineering – System of systems (SoS) considerations in life cycle stages of a system.
- [2] LR Rules and Regulations for the Classification of Ships 2004.
Available: <https://r4s.oneocean.com/regulation/document/26448>
[Accessed Feb 2024]
- [3] UK Public General Act UK Civil Contingencies Act 2004 c 36
- [4] “Merchant Shipping Act 1894 Section 7(1)(C),” 1894. [Online].
Available: <https://www.legislation.gov.uk/ukpga/Vict/57-58/60/section/7/enacted>.
[Accessed April 2018].
- [5] Boisson, Philippe (1999). Safety at Sea: Policies, Regulations & International Law. Paris: Bureau Veritas. pp.45–55.
ISBN 978-2-86413-020-8.
[Accessed July 2019]
- [6] “Merchant Shipping Act 1906. [Online].
Available: <https://www.legislation.gov.uk/ukpga/Edw7/6/48/section/7/enacted>.
[Accessed April 2019].
- [7] U.S.A Seamans Act, 4 March 1915.
[Online]. Available: <https://uslaw.link/citation/stat/38/1164>. [Accessed March 2020].
- [8] Cordes A, “Oxford University Comparative Law Forum,” 23 July 2020. [Online]. Available:
<https://ouclf.law.ox.ac.uk/conflicts-in-13th-century-maritime-law-a-comparison-between-five-european-ports/>. [Accessed February 2021].
- [9] U. Gov, “Carriage of Goods by Sea Act 1971,” 1971. [Online]. Available: <https://www.legislation.gov.uk/ukpga/1971/19/contents>.
[Accessed April 2020]
- [10] IMO, “International Safety Management Code. Code,”
[Online]. Available: <https://www.imo.org/en/OurWork/HumanElement/Pages/ISMCode.aspx>.
[Accessed 1 January 2020].
- [11] “Marine Insurance Act 1906 Section 39,” 1906. [Online].
Available: <https://www.legislation.gov.uk/ukpga/Edw7/6/41/section/39>.
[Accessed 6 April 2020].
- [12] Hague-Visby Rules - Convention of 25 August 1924 for the Unification of Certain Rules of Law relating to Bills of Lading (Treaty Series 1953, 109). Available: <http://www.dutchcivillaw.com/legislation/haguevisbyrules.htm>
[Accessed April 2020].
- [13] USS Iowa (BB-4) Navies first radio controlled ship
Available: [https://en.wikipedia.org/wiki/USS_Iowa_\(BB-4\)](https://en.wikipedia.org/wiki/USS_Iowa_(BB-4))
- [14] International Maritime Consultative Organisation (IMCO) MSC V-III/11. 9th March 1964
- [15] European Commission - CORDIS, “Final Report Summary - MUNIN (Maritime Unmanned Navigation through Intelligence in Networks),” [Online]. Available: <https://cordis.europa.eu/project/rcn/104631/reporting/en>.
[Accessed 10 July 2020].
- [16] Rolls-Royce – Remote and Autonomous Ships – The next steps.
Available: AAWA paper master v12
Accessed: January 2017

- [17] International Maritime Organization, "Regulatory Scoping Exercise for the Use of Maritime Autonomous Surface Ships (MASS) - MSC 100/5/3," International Maritime Organization, London, 2018, September 28.
- [18] International Maritime Organization, "The United Nations Convention on the Law of the Sea (UNCLOS). Available: <http://www.imo.org/en/MediaCentre/SecretaryGeneral/SpeechesByTheSecretaryGeneral/Pages/itlos.aspx>. [Accessed 28 June 2022]
- [19] Rolls-Royce plc, "Project Sisu," Rolls-Royce plc, Derby, 2017, June 20 [Online] Available: <https://www.rolls-royce.com/media/press-release/2017/20-06-2017-rr-demonstrates-worlds-first-remotely-operated-commercial-vessel.aspx>.
- [20] "Yara Birkeland Press Kit," Yara, [Online]. Available: <https://www.yara.com/news-and-media/press-kits/yarabirkeland-press-kit/>. [Accessed 10 June 2020].
- [21] Kongsberg Maritime - ASKO Project Available: https://www.kongsberg.com/maritime/feature_articles/2020/12/asko/. [Accessed April 2022]
- [22] NIPPON Foundation - MEGURI 2040 Available: <https://en.nippon-foundation.or.jp/what/projects/ocean/meguri2040> [Accessed November 2024]
- [23] Sea Machines, "The Machine Odyssey Available: <https://sea-machines.com/the-machine-odyssey-unveiling-the-journey/> [Accessed 18th January 2022]
- [24] Reach Subsea. Available: <https://reachsubsea.no/assets/reach-remote/> [Accessed April 2025]
- [25] Rolls-Royce plc, "Rolls-Royce and Finferries demonstrate world's first Fully Autonomous Ferry," 3 December 2018. [Online]. Available: <https://www.rolls-royce.com/media/press-releases/2018/03-12-2018-rr-and-finferriesdemonstrate-worlds-first-fully-autonomous-ferry.aspx>. [Accessed 18 August 2019].
- [26] International Maritime Organization, "Guidelines for the Approval of Alternatives and Equivalents As Provided for in Various IMO Instruments," International Maritime Organization, London, 2013, June 24. IMO MSC.1/Circ 1455 .
- [27] J. Molloy, S. Shahbeigi and J. A. McDermid, "Hazard and Safety Analysis of Machine-Learning-Based Perception Capabilities in Autonomous Vehicles," in Computer, vol. 57, no. 11, pp. 60-70, Nov. 2024, doi: 10.1109/MC.2024.3443751.
- [28] International Association of Classification Societies - 2020 Available: Classification-what-why-how.pdf Access: November 2023
- [29] Lloyd's Register ShipRight procedure – Autonomous Ships 2016.
- [30] ISO/IEC/IEEE 15288:2023 Systems and software engineering — System life cycle processes.
- [31] ISO/IEC/IEEE 12207:2017 Systems and software engineering — System life cycle processes.
- [32] ISO 17894:2005, Ships and marine technology - Computer applications – General principles for the development and use of programmable electronic systems in marine applications.
- [33] Lloyd's Register (LR) – ShipRight Design and Construction Digital Ships Procedure for assignment of digital Descriptive notes for autonomous and remote access ships March 2019
- [34] China Classification Society (CCS) Rules for Intelligent Ships 2024 - Effective from 1 April 2024
- [35] American Bureau of Shipping (ABS) - Autonomous and Remote Control Functions - October 2024
- [36] DNV CLASS Guideline - Autonomous and remotely operated vessels - DNV-CG-0264 Edition December 2024
- [37] ARP 4761A Guidelines for Conducting the Safety Assessment Process on Civil Aircraft, Systems, and Equipment: December 2023

- [38] Guidelines for Autonomous Shipping - Guidance Note NI 641 DT R00 E - December 2017
- [39] IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems.
- [40] Charon P, Final Results of the Paris Metro Line 1 Automation, 14th International Conference on Automated People Movers and Automated Transit Systems Apr 21, 2013. Pages 511-515
<https://ascelibrary.org/doi/book/10.1061/9780784412862>
- [41] UITP, Automated Metro Observatory 2022 Report, International Association of Public Transport, 2022.
- [42] IEC 62290-1:2014, Railway applications – Urban guided transport management and command/control systems – Part 1: System principles and fundamental concepts
- [43] UK National Audit Office, Investigation into the Watchkeeper Programme, HC 1066, 2018.
Available: <https://www.nao.org.uk/wp-content/uploads/2020/03/Defence-capabilities-delivering-what-was-promised.pdf>
- [44] Eve Air Mobility, "About Us," [Online]. Available: <https://www.eveairmobility.com>
[Accessed 8th June 2025]
- [45] Waymo, "The Waymo Driver," [Online]. Available: <https://waymo.com/waymo-driver/>
[Accessed 8th June 2025]
- [46] Reuters - "GM Cruise unit suspends all driverless operations after California ban," , Oct. 26, 2023.
Accessed 8th June 2025
- [47] B. Templeton, "The 10 Billion Dollar Question for Robotaxis," Forbes, 2023.
- [48] UK Government, Automated Vehicles Act, 2024.
- [49] UITP – Available: https://cms.uitp.org/wp/wp-content/uploads/2020/06/Statistics-Brief-Metro-automation_final_web03.pdf
[Accessed March 23]
- [50] M. C. Erturk, H. Jamal and D. W. Matolak, "Potential Future Aviation Communication Technologies," 2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC), San Diego, CA, USA, 2019, pp. 1-10, doi: 10.1109/DASC43569.2019.9081679.
Available: <https://ieeexplore.ieee.org/author/37270693400>
[Accessed May 2025]
- [51] L. D. Earley, "Communication in Challenging Environments: Application of LEO/MEO Satellite Constellation to Emerging Aviation Networks," *2021 Integrated Communications Navigation and Surveillance Conference (ICNS)*, Dulles, VA, USA, 2021, pp. 1-8, doi: 10.1109/ICNS52807.2021.9441549.
- [52] A. Mirabadi, N. Mort and F. Schmid, "Design of fault tolerant train navigation systems," *"Proceedings of the 1999 American Control Conference (Cat. No. 99CH36251)*, San Diego, CA, USA, 1999, pp. 104-108 vol.1, doi: 10.1109/ACC.1999.782749.
- [53] Kelly Review into the circumstances related to the closure of Heathrow Airport on 21 March 2025
Available: Kelly Review published
Access: March 25
- [54] ISO/PAS 8800:2024(en) - Road vehicles — Safety and artificial intelligence.`
- [55] Burmeister H-C, Bruhn W, Rødseth ØJ, Porathe T. Autonomous unmanned merchant vessel and its contribution towards the e-navigation implementation: the MUNIN perspective1. *Int J E-Navig Marit Econ* 2014;1:1–13.
<http://dx.doi.org/10.1016/j.enavi.2014.12.002>. `
- [56] Kretschmann L, McDowell H, Rødseth ØJ, Fuller BS, Noble H, Horahan J. Maritime unmanned navigation through intelligence in networks– quantitative assessment; 2015.
- [57] Rødseth ØJ, Burmeister H-C. Risk assessment for an unmanned merchant ship. *TransNav Int J Mar Navig Saf Sea Transp* 2015; 9:357–64. <http://dx.doi.org/10.12716/1001.09.03.08>.

- [58] Lee P, Theotokatos G, Boulougouris E, Bolbot V. Risk-informed collision avoidance system design for maritime autonomous surface ships
<https://doi.org/10.1016/j.oceaneng.2023.113750>
- [59] Chaal, M., Ren, X., BahooToroody, A., Basnet, S., Bolbot, V., Banda, O. A. V., & Gelder, P. V. (2023). Research on risk, safety, and reliability of autonomous ships: A bibliometric review. *Safety Science*, 167, Article 106256. <https://doi.org/10.1016/j.ssci.2023.106256>
- [60] Dreyer L, Ottedal H (2019). Safety Challenges for Maritime Autonomous SURFACE SHIPS: A Systematic Review Proceedings of Ergoship 2019. Western Norway University of Applied Sciences.
<http://hdl.handle.net/11250/2638416>
- [61] Fjørtoft K, Mørkrid O E. Resilience in Autonomous Shipping
Conference Paper · January 2021
DOI: 10.3850/978-981-18-2016-8_470-cd
- [62] Centre for Assuring Autonomy (CfAA) Systematic literature review DSTA preliminary findings. May 2025
- [63] Centre for Assuring Autonomy (CfAA) Guidance on the Safety Assurance of Autonomous Systems in Complex Environments (SACE). July 2022.
- [64] Centre for Assuring Autonomy (CfAA) Guidance on the Assurance of Machine Learning in Autonomous Systems (AMLAS). March 2021.
- [65] Z. Porter, P. Ryan, P. Morgan, J. Al-Qaddoumi, B. Twomey, J. McDermid, and I. Habli, "Unravelling Responsibility for AI," arXiv preprint, arXiv:2308.02608, Aug. 2023.
- [66] Burton S, Habli I, Lawton T, McDermid J, Morgan P, and Porter Z, "Mind the Gaps: Assuring the Safety of Autonomous Systems from an Engineering, Ethical, and Legal Perspective," *Artificial Intelligence*, vol. 279, p. 103201, 2019.
- [67] International Maritime Organization, International Maritime Organization, "International Convention for the Safety of Life at Sea (SOLAS), 1974," [Online]. Available: [http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-\(SOLAS\),-1974.aspx](http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx). [Accessed 10th June 2019].
- [68] European Union Aviation Safety Agency (EASA) - AMC and GM to Part ATCO MED March 2015 Available: <https://www.easa.europa.eu/en/document-library/acceptable-means-of-compliance-and-guidance-materials/group/part-atcomed#part-atcomed> [Accessed March 2019]
- [69] European Union Aviation Safety Agency (EASA) – Doc 9859 Safety Management Manual 2018.
- [70] BSI – PD/ISO/PAS 21448:2019 - Road vehicles — Safety of the intended functionality ISBN 978 0 580 94502 1
- [71] Leveson NG. Engineering a safer world— systems thinking applied to safety. Cambridge, MA: MIT Press; 2011.
- [72] Institute of Mechanical Engineers – safety and Reliability Group – ALARP for Engineers – May 2024
- [73] Osborne M, Hawkins R. Defining an Effective Context for the Safe Operation of Autonomous Systems - Assuring Autonomy International Program, University of York
- [74] ISO 26262 – Road Vehicles – Functional Safety - 2018
<https://www.iso.org/obp/ui/en/#iso:std:iso:26262:-1:ed-2:v1:en>
- [75] ARP 4754A Guidelines for Development of Civil Aircraft and Systems.
- [76] ISO 31000:2018 Risk management — Guidelines - Edition 2, 2018)
- [77] Safety Critical Systems Club (SCSC) – Publication 159 – Assurance Case Guidance
- [78] R D Alexander, R D Hawkins, T P Kelly - from Safety Cases to Security Cases – Safety Critical Systems Club 2017.

- Available: <https://www-users.york.ac.uk/~rda2/SSS%20'17%20Alexander%20Hawkins%20and%20Kelly.pdf>
[Accessed: February 2019]
- [79] R Hawkins, T Kelly, J Knight, and P.Graydon. . A New Approach to Creating Clear Safety Arguments
Available: <https://www-users.york.ac.uk/~rdh2/papers/HawkinsSSS11.pdf>
 - [80] Kelly, T.P., McDermid, J.A. (1997). Safety Case Construction and Reuse Using Patterns.
In: Daniel, P. (eds) Safe Comp 97. Springer, London. https://doi.org/10.1007/978-1-4471-0997-6_5
 - [81] ISO/IEC Guide 51:2014 Safety aspects — Guidelines for their inclusion in standards
 - [82] T Kletz Process Plant – A Handbook for Inherently Safer Design. ISBN: 9781439804551
 - [83] Office for Nuclear Regulations – Safety Assessment principles for Nuclear Facilities 2014 Edition, Revision 1 – January 2020
 - [84] Health and Safety Executive – Reducing Risk – Protecting People - ISBN 0 7176 2151 0
 - [85] Dynamic Safety Cases for Through-life Safety Assurance
<https://ntrs.nasa.gov/api/citations/20150011054/downloads/20150011054.pdf>
 - [86] IMO RESOLUTION A.893(21) - Guidelines for Voyage Planning - adopted on 25 November 1999
 - [87] International Maritime Organization, “International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, 1978,” [Online].
Available: <http://www.imo.org/en/OurWork/HumanElement/TrainingCertification/Pages/STCW-Convention.aspx>.
[Accessed 5th June 2019].
 - [88] Freeman.R: A Stakeholder Approach ISBN 978-00521-15174-0 Cambridge University Press.
 - [89] OECD/NEA Forum on Stakeholder Confidence.
https://www.oecd-neo.org/jcms/pl_26865/forum-on-stakeholder-confidence-fsc
 - [90] IAEA, Handbook on Nuclear Law, IAEA, 2003. ISBN 92-0-105703-2
 - [91] Mitchell RK, AGLE BR, Wood DJ - Toward a Theory of Stakeholder Identification and Salience: Defining the principle of who and what really counts
Academy of Management Review 1997, Vol. 22, No. 4, 853-886.
 - [92] Neville BA, Bell S - Stakeholder Salience Reloaded: Operationalising Corporate Social Responsibility
ANZMAC Conference Proceedings – Adelaide 1-3 Dec 2003 – 1883 - 1889
 - [93] <https://www.hse.gov.uk>
 - [94] Lloyds Register Rules and Regulations for the Classification of Ships
Available: <https://r4s.oneocean.com/regulation/page/284644>
Accessed: June 2025
 - [95] IMO MSC 108/19 Comments on the review of the North Atlantic wave data
 - [96] IAEA Safety glossary terminology used in nuclear safety and radiation protection 2018 edition
 - [97] ISO TS 23860 ISO/TS 23860:2022 Ships and marine technology — Vocabulary related to autonomous ship systems
 - [98] ISO 45001:2018 Occupational health and safety management systems — Requirements with guidance for use
 - [99] Merryman, J (1969). The Civil Law Tradition: An Introduction to the Legal Systems of Western Europe and Latin America. Stanford University Press. p.1. ISBN 9780804706940.
 - [100] The Law Dictionary – Available: <https://thelawdictionary.org/system/>
[Accessed November 2023]
 - [101] International Atomic Energy Association (IAEA) Safety Standards – Safety assessment for Facilities and Activities
General Safety Requirements – No GSR Part 4 (Rev 1)
 - [102] Defence Safety Authority – DSA 02 – DMR: Defence Maritime Regulator for Health, Safety and Environmental Protection 2025
Available: https://assets.publishing.service.gov.uk/media/672a462f541e1dfbf71e8bea/DSA02-DMR_2025_Edition_-_Defence_maritime_regulations_for_health_safety_and_environmental_protection.pdf
[Accessed: May 2025]

- [103] B.Twomey, "SYSTEM DESIGN AND INTEGRATION," and 'The Cyber Enabled Ship'in
ENCYCLOPEDIA OF MARITIME AND OFFSHORE ENGINEERING, John Wiley&Sons, 2010.
<https://www.wiley.com/en-gb/Encyclopedia+of+Maritime+and+Offshore+Engineering> –
p-9781118476352
- [104] Oginni D, Camelia F, Chatziichailidou M, Ferris TIJ - Applying System-Theoretic Process Analysis (STPA)-based
methodology supported by Systems Engineering models to a UK rail project.
Safety Science Vol 167 November 2023 - <https://doi.org/10.1016/j.ssci.2023.106275>
- [105] Leveson, N. G., & Thomas, J. P. (2018). STPA handbook. Cambridge, MA, USA, 1-188
- [106] International Atomic Energy Association (IAEA) Safety Standards – Safety of Nuclear Power Plant Design
Specific Safety Requirements – No SSR -2/1 (Rev.1)
- [107] Lloyds Register Advisory - Ship Emergency Response.
Available: <https://www.lr.org/en/services/advisory/operational-services/ship-emergency-response/>
[Accessed: June 2025]
- [108] IEC 60947 Ed 6 2020-04 Low Voltage Switchgear and Control gear – Pt 1: General Rules
- [109] International Maritime Association – MSC 109/WP8
- [110] Acquisition Safety and Environmental Management System – SMP 12 – Safety Case Report – System Revision ID 5035 –
ASEMS Document Version 4.6
- [111] Kelly TP, McDermid JA. A systematic approach to safety case maintenance –
Reliability Engineering and Systems Safety Vol 71, Issue 3, March 2001, Pages 271-284
[https://doi.org/10.1016/S0951-8320\(00\)00079-X](https://doi.org/10.1016/S0951-8320(00)00079-X)
- [112] Safety Critical Systems Club (SCSC) Assurance Case Working Group – Goal Structuring Notation Community Standard
Version 3 (SCSC 141C) May 2021.
- [113] Habli I, Hawkins R, Paterson C, Ryan P, Jia Y, Sujan M, McDermid J. – Centre for Assuring Autonomy –
The BIG Argument for AI Safety Cases.
Available: [https://www.york.ac.uk/media/assuring-autonomy/documents/
The%20BIG%20Argument%20for%20AI%20Safety%20Cases%20\(1\).pdf](https://www.york.ac.uk/media/assuring-autonomy/documents/The%20BIG%20Argument%20for%20AI%20Safety%20Cases%20(1).pdf)
[Accessed: March 2025]
- [114] M Lutzhoft, J Earthy, Hynnekleiv A, Petersen ES - Human-centred maritime autonomy - An ethnography of the future
J. Phys.: Conf. Ser. 1357 012032
- [115] MGN 703: Information concerning the training and competence of Remote Operators working with
Remotely Operated Unmanned Vessels (ROUVs), certified under the Workboat Code Edition 3
Published 30 October 2024
- [116] Edmundson A, Twomey B. Systems Engineering – The Hard Way - Conference: 14th International
Naval Engineering Conference and Exhibition October 2018
DOI:10.24868/issn.2515-818X.2018.009
- [117] BS EN ISO 9001:2015+A1:2024 – TC Quality management systems. Requirements Current
Published: 30 Sep 2024
- [118] ISO/IEC/IEEE 90003:2018 Software engineering — Guidelines for the application of ISO 9001:2015 to computer software
Edition 1 2015
- [119] ISO/IEC 25000:2014 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE)
Guide to SQuaRE. Ed 2, 2014.
- [120] Foreign flagged ships detained in the UK during March 2022 under Paris MOU
Available: [https://www.gov.uk/government/news/foreign-flagged-ships-detained-in-the-uk-during-march-2022-
under-paris-mou](https://www.gov.uk/government/news/foreign-flagged-ships-detained-in-the-uk-during-march-2022-under-paris-mou)
- [121] SKULD – Good Anchoring Practices, Available: <https://www.skuld.com/topics/ship/safety/good-anchoring-practice/>
[Accessed March 2022]
- [122] Endsley MR. Article in Human Factors – The Journal of the Human Factors and Ergonomics Society – March 1995 37(1) 32-64

- [123] Parasuraman R, Manzey D. Complacency and Bias in Human Use of Automation:
- [124] Ministry of Infrastructures and Transports - Marine Casualties Investigative Body
Cruise Ship - COSTA CONCORDIA. .Marine casualty on January 13, 2012 - Report on the safety technical investigation
- [125] Panama Maritime Authority Directorate General of Merchant Marine Maritime Affairs Investigation Department
M/V "EVER GIVEN" IMO No. 9811000 - R-026-2021-DIAM - Casualty Date: March 23rd, 2021
- [126] Marine Accident Investigation Branch – Solong and Stena Immaculate Interim Report 3rd April 2025
- [127] UK Public General Acts - Marine Insurance Act 1906
1906 c. 41 (Regnal. 6_Edw_7)
- [128] IMO, "ISM Code," [Online]. Available: <https://www.imo.org/en/OurWork/HumanElement/Pages/ISMCode.aspx>.
[Accessed 1 January 2020].
- [129] B. Twomey, "Autonomy, A Vision or Reality," Royal Institute of Naval Architects, WARSHIP 2025, International conference, Glasgow.
- [130] B Soyer, A Tattenbom, D Leloudas. – Remote Controlled and Autonomous Shipping – UK Based Case Study – January 2022
- [131] IACS Classification Societies – Their Key Role
<https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/05/09132413/classification-societies-key-role.pdf>
[Accessed October 2025]
- [132] SAEJ0316 202104- Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles
https://www.sae.org/standards/j3016_202104-taxonomy-definitions-terms-related-driving-automation-systems-road-motor-vehicles
[Accessed September 2025]
- [133] North Sea Memorandum of Understanding
<https://smartmaritimenetwork.com/2023/09/19/denmark-uk-and-belgium-sign-autonomous-vessel-testing-mou/>
[Accessed September 2025]
- [134] WMU Journal of Maritime Affairs: Human element in autonomous shipping: a study on skills and competency requirements – April 2025
<https://link.springer.com/article/10.1007/s13437-025-00366-9>
[Accessed October 2025]
- [135] A McLellan – Maritime digital skills lacking but industry catching up – IMarEST – March 2025
<https://lhttps://www.imarest.org/resource/mp-maritime-digital-skills-lacking-but-industry-catching-up.html>
[Accessed October 2025]
- [136] Australian Maritime Agency (AMSA) Policy on regulatory treatment of uncrewed and/or autonomous vessels – 20 February 2020.
<https://www.amsa.gov.au/vessels-operators/domestic-comm>
[Accessed November 2025]
- [137] Norwegian Maritime Authority (NMA)- Guidance in connection with the construction or installation of automated functionality aimed at performing unmanned or partially unmanned operations –Circ – Series V – RSV12 - 2020
27 08 2020.
- [138] Danish Maritime Authority (DMA)– Principles and Procedures for approval of MASS – Version 2
24 06 2021.
- [139] UK Maritime and Coastguard Agency (MCA) – Certification process for vessels using innovative technology -MGN 664 (M+F)
March 2022.
- [140] Operator-Centred Enhancement of Awareness in Navigation (OCEAN) - Horizon Europe, CL5-2022-D6-01 – Grant agreement 101076983
May 2025.

Chapter 10 : Appendix A.

RINA WARSHIP 2025 Conference – Glasgow – The Future Fleet: Sustainability and Autonomy

The Author published a paper for the Session on Autonomy: ‘Autonomy – A Vision or Reality’, which explored *the principles of ‘Inherent Safety, Fault Tolerant and Layers of Protection’ in the context of the MAI, and how these principles influence the design within a dynamic safety case, challenging legal framework and changing stakeholder community depending on the operational requirements of the MAI’.*

The presentation generated several questions from the audience indicating both engagement with and relevance of the research within the maritime and defence sectors. Selected questions and academic responses are summarised below:

- **Is the Lifecycle Process Model (LPM) scalable across different vessel types and operational contexts?**

Yes. The LPM has been intentionally designed with scalability as a foundational requirement. It adopts a modular, stage-based structure that can be tailored to different system complexities and mission profiles. The model is not prescriptive in terms of system architecture or vessel size; rather, it provides a structured framework for risk identification, stakeholder engagement, and assurance development applicable to both low-complexity commercial vessels and high-complexity naval platforms.

- **Can the models be applied to naval applications, including those operating under military exemptions?**

Yes. While naval vessels may operate under exemptions to statutory regulations (e.g., SOLAS exemptions under UNCLOS provisions), it is generally accepted practice that they achieve a level of **‘at least as good as statute’** in non-combat conditions. The frameworks developed in this thesis, including the LPM, SPM, and MAI DE, provide a structured basis for demonstrating ‘Acceptably Safe’ operations regardless of the legal classification of the vessel. Their adaptability to mission-specific requirements and operational doctrines makes them

suitable for application in naval contexts, particularly for tasks involving logistics, humanitarian aid, or other non-combat operations where civilian safety expectations and regulatory engagement still apply.

Comments from GE Marine Engine Service.

In addition to the academic and regulatory evaluations, practical insights were also provided by industry practitioners, including GE Marine Engine Service, who offered feedback based on initial applications of the Lifecycle Process Model (LPM) within their operational context.

“Having utilised the lifecycle process model, I have started to incorporate it into field service actions at GE to identify risk interfaces and inform shipyard planners. This has helped to address potential items that cause delays in construction and impede timely completion of OEM milestones.” - Mr ABC - Director Marine Engine Services.