Safety of Autonomous Shipping

Paul James BEng CEng MRINA WhSch RCNC(Hon) (lead author) Lloyds Register EMEA
Anderson Chaplow BEng AMRINA Lloyds Register EMEA
Matthew Palmer BEng CEng MIMechE Lloyd's Register EMEA

Synopsis

With current and expected developments in unmanned and autonomous systems, LR envisages that within the near future, Unmanned Marine Systems (UMS) will enter into widespread use through many sectors of the maritime industry. Five years ago, we developed the LR Unmanned Marine Systems Code in conjunction with industry to help set out a regulatory framework. It was developed to provide a unique and valuable assurance process to certify the safe design, build and maintenance of UMS to achieve certification which is acceptable to Flag States, local regulators and other parties. LR has applied the code process and framework to a number of UMS projects and is developing a unique understanding of the challenges associated with the technology. Companies involved in producing equipment are often not familiar with marine assurance processes nor the risks and hazards in the marine environment and the rapid development times mean that the equipment may not be appropriate or have the required level of integrity. In this paper, LR will share the experience of applying the Code for UMS.

Keywords: Safety Assurance Autonomy Code Unmanned

1 Introduction

With developments in autonomous and remote systems and the reality of Unmanned Maritime Systems (UMS) being trialled and deployed in many sectors of the maritime industry, Lloyd's Register (LR) has been looking at how it can support the industry in demonstrating safe design and quality of manufacture.

The current maritime regulatory framework was developed on the basis of mitigating the risks for vessels that have crew. The risks for the operation of UMS differ significantly from those for a crewed vessel and so any equivalent regulatory framework developed for UMS needs to take this into account.

With this in mind, Lloyd's Register developed a code to provide a framework for the assurance of safety [LR 2017], mitigating risks for UMS. This code was written to work alongside evolving requirements for safe operation and environmental protection. It provides a complete regulatory framework for UMS that is equivalent to that for manned vessels.

The LR Code for Unmanned Marine Systems was published in 2017 and is applicable to all autonomous and remote controlled systems operating above and below the water surface. The application of the Code is dependent upon the owner defining their operational requirements and risk tolerance, which will then determine the safety, and commercial risks that are applicable; hence tailoring how the Code for UMS is applied. The scope is wider than that currently covered by Classification Rules as it is written to cover all areas of SOLAS that are applicable to UMS and includes any shoreside control arrangements.

In parallel with the development of the Code for UMS, LR has been working with several suppliers of UMS, to certificate their vessels using the Code for UMS and we have issued vessel certificates on a range of UMS systems. The UMS vessels certificated are designed to carry out subsea positioning, surveying, autonomy test bed and environmental monitoring tasks in offshore and coastal waters.

Author's Biographies

Paul James Joined Lloyd's Register in 1994 after graduating from Southampton University with a degree in Naval Architecture. He was part of the team which developed LR's Naval Ship Rules and has since been involved in their application to a wide variety of projects such as Type 26, Type 31, QEC, Type 45, Type 23, and other projects such as NSRS Dreadnought and Astute. He manages the Naval Centre of Expertise in Bristol responsible for delivering classification, assurance and certification of ships, submarines and autonomous vessels.

Anderson Chaplow is a Lead Specialist in the Lloyd's Register's Naval Centre of Expertise in Bristol. He and his team are responsible for developing and delivering the LR Code for Unmanned Maritime Systems to industry and supporting regulators and clients with the development and application of assurance techniques for naval platforms, unmanned and autonomous technologies. Anderson has been with Lloyd's Register for nearly seventeen years with previous roles in the survey and certification of equipment & components, complex new construction projects and existing vessel surveys.

Matthew Palmer joined LR in 2012 after his previous role in the Royal Navy as an Engineering Office on Trafalgar Class submarines. Matthew works on developing Goal-based Standards, Rules and assurance products for naval submarines and unmanned marine system assurance products. Matthew is also the part of the Secretariat for the INSA Naval Ship and Submarine Code. Matthew has been leading the industry engagement, on the certification of unmanned marine systems under 24m.

Images thanks to Fugro, IXblue, ASV and BAE systems

Figure 1 Types of craft assessed

2 Regulatory Framework

Looking at the regulatory framework that has evolved for ships, and with reference to Figure 2; regulatory requirements may be broadly broken down into those covering: safe design, environmental protection, and safe operation.

The goal of the Code for UMS is to be able to assure the safe design, build and maintenance of UMS against a common framework that minimises the effort required by an owner or operator to present a robust safety argument which can be used to then achieve certification or an exemption from a regulator. Currently there no regulations for UMS and LR through its UMS certification process has been supporting a number of Flag States to allow them to issue exemptions from legislation which require robust safety arguments. This relationship between the LR and the Regulator (Flag State) is a key consideration in any UMS project and it should be agreed right at the start of a project, together with the scope of LR and Flag verification activities. As the industry matures, LR expects to incorporate these Regulator requirements into its UMS Code on a country by country basis.

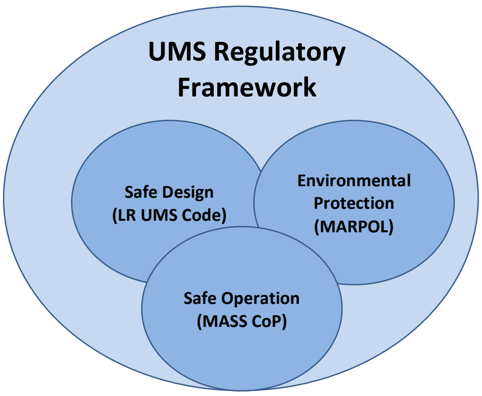

Figure 2: UMS Regulatory Framework

Safe operation and environmental protection are outside the scope of the Code for UMS. The requirements for safe operation have been developed by the UK Marine Industry Alliance within the Maritime Autonomous Ships Regulatory Working Group which is a group of key UK industry representatives established to develop the UK position on regulation and which has the support of the MCA. They have published a Maritime Autonomous Surface Ships (MASS) UK Industry Code of Practice [MARI UK 2021].

For Environmental protection it is considered that the requirements of MARPOL [IMO 1978] should be broadly applicable as written. Some interpretation may be required which can be addressed by a separate environmental risk assessment.

3 Unmanned Systems Code

3.1 Structure of the Code for UMS

The Code for UMS has been written using a goal-based structure. It provides a minimum level of safety for UMS and a method to define and assess against the owner or operator's declared tolerability of risk for loss or damage to the asset. The benefits to the designer of using the goal-based structure are that it defines an ultimate safety objective whilst allowing for the consideration of alternative designs and solutions that meet the safety objective; thereby supporting innovation in an area that is developing fast. [James 2014] [Hoppe 2008]

The structure of the code is similar to that used for ANEP 77 The Naval Ship Code [INSA 2020], a safety code which is written as a naval equivalent to SOLAS, the development and implementation of which, Lloyd's Register has been contributing to. With reference to Figure 3; the tiers of the Code for UMS are as follows, with the increasing width of lower tiers representing increased level of detail:

- Tier 0 is the overall Aim of the Code for UMS which is that "The Unmanned Marine System (UMS) shall be safe, reliable, capable and resilient in all Foreseeable Operating Conditions." The extension from just safe operation alone is deliberate and an intended aim of the Code.
- Tier 1 defines high level Goals for each hazard area, and these form the chapters of the Code for UMS. These Goals align to the overall Aim of the code.
- Tier 2 Functional Objectives provide the criteria to be satisfied in order to meet the Tier 1 Goals.
- Tier 3 Performance Requirements define a more detailed set of requirements to meet Tier 2 Functional Objectives and are qualitative to allow them to be met by a range of solutions.
- Tier 4 Solutions will describe the design solution, how it is to be verified and needs to be justified against the Tier 3 Performance Requirements to show it is adequate. Tier 4 solutions are not defined within the Code for UMS. This is because of the potential diversity in design and operation of UMS. The Code expects an appropriate solution be selected from a combination of: Classification Rules, National or International Codes and Standards or where standards do not exist, or are not appropriate, through the application of risk based assessment methodologies that demonstrate the performance requirements are achieved.

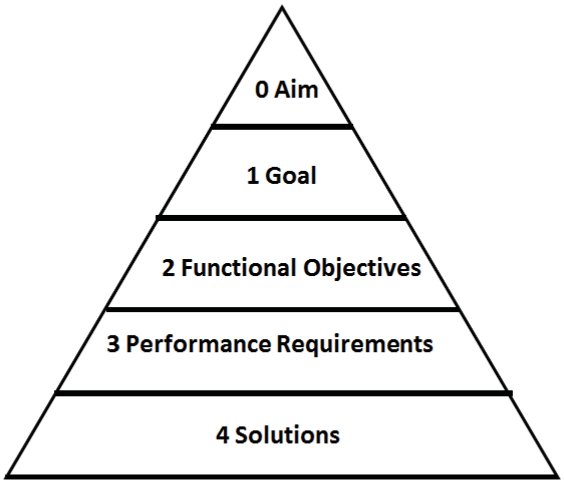

Figure 3: Code for UMS Structure

For the Code for UMS to cover safe design and operation in its entirety, we must first establish what the risks are which occur from the operation of UMS and include these in a framework which can then ensure they are adequately controlled and mitigated. For the Code for UMS, this is achieved through the development of a concept of operations (ConOps) which informs the assurance process.

Within the Code for UMS the designer can specify their own tolerance level for the risk of loss or damage to the UMS and so where required, can enhance the level of integrity above the minimum level defined for safety.

3.2 Scope of the Code for UMS

The Code for UMS will cover all aspects of safe design for autonomous and remote-controlled UMS operated on or below the surface. It therefore covers all aspects of SOLAS [IMO 1974] that are applicable to unmanned vessels and the additional hazards resulting from the way that UMS are operated.

The Goals, Functional Objectives and Performance requirements have been divided into the following hazard areas forming the main technical chapters of the Code for UMS:

Structure

- Stability
- Control System
- Electrical System
- Navigation System
- Propulsion and Manoeuvring

- Fire
- Auxiliary Systems

The scope and boundary of each hazard area is defined together with its interaction with other hazard areas to provide clarity of what is to be covered when carrying out an assessment.

The Functional Objectives and Performance Requirements are written to cover identified hazards relating to the operation of UMS. To ensure completeness, these have been validated against existing sources of requirements in Conventions, Codes and standards.

The Code for UMS is limited to the design of the UMS system alone, and so it does not cover any safety, environmental and commercial risks resulting from embarked cargo or mission specific equipment. These can be covered through separate hazard identification and risk assessment techniques. The Code for UMS covers the design of the UMS for safe operation and maintenance but does not address operator training and qualification. If the UMS is occasionally manned, carries dangerous goods or harmful substances all other relevant Codes and Conventions must also be complied with.

4 Application of the Code for UMS

LR have been through a number of iterations of the assurance process using the Code for UMS. The code is a goal based standard and whilst we understood what was needed to deliver a safety argument for certification, we were working in a market sector which had not yet considered the challenge of assurance or what this might entail for them as designers and operators. It is fair to say that the naval sector had a better understanding of what was required.

We have now settled on an approach that allows us to lead stakeholders through a process which establishes: the project and certification requirements, the assurance path for achieving these, the verification activities required, development of evidence, final review and certification. These five stages are shown in Figure 4.

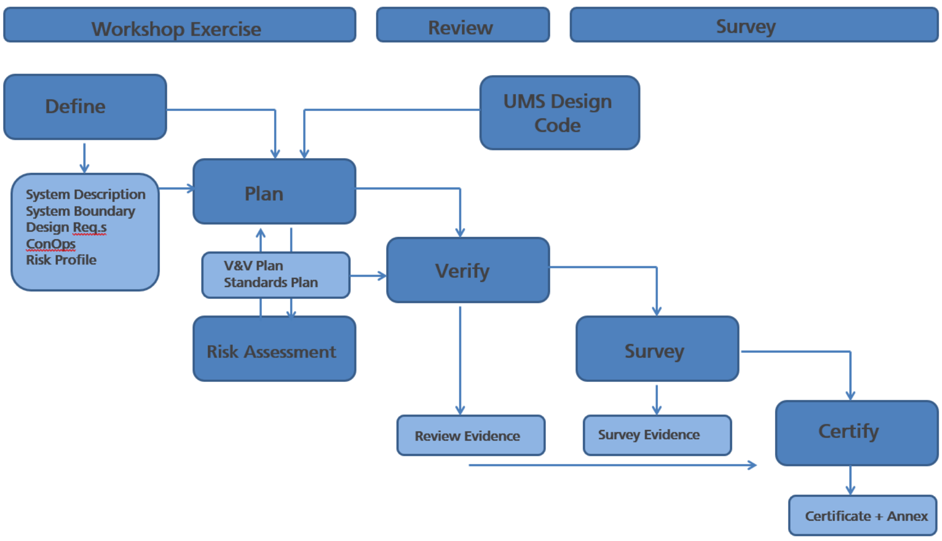

Figure 4: UMS Assurance Process Stages

The process is not necessarily novel, but it is an approach that recognises that a reasonable proportion of an unmanned boat is the same as a manned boat and allows the depth and rigor of assurance to be tailored to suit the operational risk profile as established by the Concept of Operations.

4.1 Requirements Setting

The Code requires the operational context of the vessel to be defined in a document called a concept of operations (ConOps). The ConOps defines the key characteristics and functions of the vessel, the operating environment, reversionary modes and the level of automation. This provides the context for the subsequent assessment of the UMS system and we have developed a template that aims to draw out the key characteristics and functions of the vessel. The majority of craft certified to date have been remote controlled or closely supervised systems with a human in the loop.

It is surprising how many projects did not have a clear and comprehensive concept of operations and the workshops held with clients to derive the document required by the Code for UMS have helped the owner and regulator understand the boundaries of operation and the implications of their vessel requirements. In many cases establishing these boundaries has helped reduce the work involved in safety justification. For example, a small slow moving supervised craft may not need a high integrity assurance of propulsion and steering because it cannot become a hazard and can be quickly recovered.

Writing the ConOps means that operating limitations are clearly identified but more importantly, the impact of these constraints are understood, both on the final operations but also on the assurance requirements needed to prove them.

The ConOps informs the assurance of the vessel and as such it becomes an essential part of the final Code for UMS Certificate. Through-life, its continued validity will be confirmed.

4.2 Assurance Plan

With the ConOps established we can plan out the assurance process to be applied for the different elements or components of the system.

As a part of the initial workshop we apply a modified Technology Qualification process which implements a system decomposition process for the UMS and assesses each of the components against three criteria: technology readiness, operational readiness and integration maturity. Initially using simple filters each component is categorised according to a screening matrix using a ‘Red, Amber, Green’ approach – represented in two dimensions in Figure 5.

Components in the Red category are considered to be introducing a high level of new technical uncertainty and are therefore subject to a high level of qualification review which include: testing, risk assessment, mitigation, and potential design change. Components in the Yellow category, presenting a lower level of uncertainty, will be subject to a subset of qualifications expected for the red category.

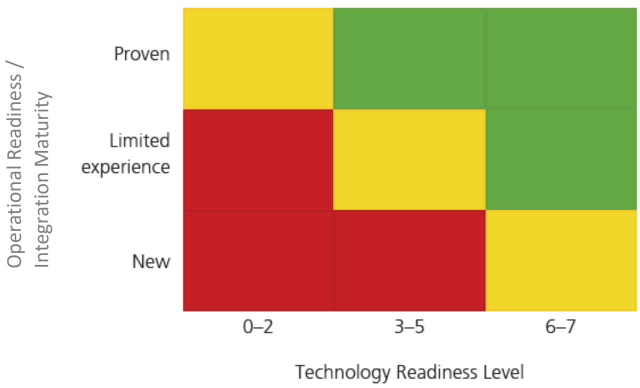

Figure 5: Initial Screening Matrix

For each of the components assessed as red, a risk assessment is required. This process is carried out to ensure that all reasonably foreseeable hazards associated with a particular technology or component are identified and adequately controlled.

Each component is also identified and reviewed individually together with its system interactions to determine the consequence (and likelihood) of failure in order to establish the required level of rigour for assurance. The term “failure” may also include unintended operation.

This is based on a Level of Integrity approach which asks five key questions. If the component or system fails, what is the consequence for:

- people on board,
- people/objects in the vicinity,
- the environment,
- the operability or capability of the system and
- the survivability of the system.

The outcome of this screening establishes whether we require a first, second or third party review of the particular system in question.

This process can be difficult to apply, subjective and we have found ourselves in some interesting discussions with regulators at various points. However, the process is required to ensure that the assurance provided is proportionate to the cost, size and risk profile of small vessels which we are currently certifying. We recognise that this step will become less relevant as vessel size and risk increases.

As discussed, one of the challenges with these vessels is the combination of manned and unmanned operations. Application of manned requirements is clear for vessels designed to carry people, but if this is intended only as a periodic or occasional function, such as for trials, vessel repositioning or transit of restricted waters, application of the traditional standards becomes difficult, particularly for vessels intended to have unrestricted operation in the unmanned mode but restricted operation in the manned mode.

4.3 Verification

The output of the Assurance stage is a Verification Plan which will include the following methods of assurance.

- Design review
- Component Certification
- Construction survey
- System Installation survey
- Tests and trials
- In service survey

The Code for UMS defines verification activities appropriate for each level of integrity (LoI). For design review activities, suitable standards will need to be identified and applied. As discussed these may need to be tailored if people are not onboard.

This Verification Plan becomes the source of reference regarding verification activities to be carried out during the design build and testing of the vessel including details of milestones and checkpoints for review and the documentary evidence to be provided.

The verification activities will have a cost associated with them and this must be factored into any programme, whilst limited verification may be undertaken for prototyping and trials, selling these vessels on the open market requires a robust safety argument with sufficient verification to satisfy the regulator. We have found that designers have not considered these costs, in particular for software where the ConOps and system function demand a high level of integrity (SIL2 for example).

Code development and software quality procedures plus 3rd party verification will add cost to software development. This cost is significantly increased when there is an “uncertain” part of the code and machine learning is introduced. This may be within the main control system or individual sensors (optical processing) which might not be obvious. At the present time, machine learning cannot be used in safety critical systems as we have no formal process for verification.

Requirements for software integrity can be addressed through redundancy. We have often seen duplication of hardware and software and whilst this provides redundancy, it does not provide diversity and identical single points of failure in the duplicated systems may still exist. Diversity in vessel communication systems, Estops and heartbeat systems have gained particular focus in our verification activities. Communications systems may have pauses or delays in receipt of data and transmission of commands therefore the reliability and latency of communication systems must be considered in any safety argument.

We have often required a significant focus on the sensor suite. The human body is a remarkable machine and adept at processing: optical, motion, audio, tactile and olfactory inputs, combining them with experience to make appropriate decisions. Several key questions need to be asked.

- Which signals do we need to replicate at the control centre to make an equivalent decision?
- What is the appropriate sensor suite required to enable safe navigation?
- Can the sensors be confused by the environment? and
- Do we need reversionary means?

Note that in these certification examples the focus is less on the marine engineering (hull, engines, pumps, piping, propulsors) and more on the control system and sensor suite. From our experience the Code for UMS assurance process has been shown to provide the right focus as it is concentrating assurance effort on those areas which pose the greatest risk and which have greatest uncertainty.

Fortunately, we have been able to work with some designers with significant experience in testing and operating these vessels, this has provided significant confidence in their systems. What is generally true however is that the focus of their efforts has been on getting the system to work and to market. They have not necessarily considered the 'design for assurance' requirement that might assist in enabling them to present a coherent argument on how or why something is appropriate and acceptable.

In some cases the development of the operating system has missed basic marine 'truths' and the vessel systems or the limitations of these systems has not been appropriately integrated, for example using speed as a set point and not engine RPM which results in continuous engine hunting. We have also seen this in the development of some COLREGs algorithms which do not include appropriate input from skilled navigators.

4.4 Evidence Gathering

The certification case is based on evidence, most builders still have a way to go with documentation, particularly system descriptions. To date we have used a variety of sources in order to support our evidence reviews - operator manuals being one of the more useful but also operating logs and bills of materials.

Designers using agile development processes which tweak and adapt software applications as they go, can mean we lose sight of the basis of design and the ability to describe or explain a system in a logical way. This may require retrospective specification of software requirements or formalisation of baseline module acceptance and application of traditional management techniques for future development.

Software quality as discussed, is a challenge, ensuring we have the appropriately qualified and experienced persons developing the software from the beginning. A lot of UMS software has evolved from lab tests and experiments with patches to fix emergent issues. Whilst the software is subject to a test environment this may not have adequately stretched the software and found its limitations. We may have always tested in good weather with well-functioning sensors and not adequately tested the software with a degraded or confused environment with aged or degraded sensors. Something several autonomous vehicle operators are discovering [Zhou 2017]

For most remote control systems we can avoid some of the more difficult questions around the assurance of autonomy. The majority of our certification reviews so far have seen safe operation established through diverse and redundant means of establishing control, via independent e-stop systems or by establishing direct control over the system drives by alternate diverse means.

A final point is particularly important, and that is about ensuring that the residual design risk is appropriately transferred to the operator in a way that they can understand. That ‘handshake’ must enable the operator to complete the hierarchy of controls in a way that satisfies the overall safety argument. Put in simple terms, does the operator really react and respond as the designer assumed.

Where we do not yet have the technology, or confidence to control the risk within the design, which is the case with a lot of autonomous technology, we are relying more on operational controls - and these must be appropriate and safe, documented and tested in service recognising the human element.

4.5 Certification

The final stage is a review of the available evidence against the Goals and Performance Requirements of the Code for UMS. The review is progressive, beginning shortly after the development of the Verification Plan as design review activities and survey activities are completed, and evidence generated. The last pieces of evidence will be generated from sea trials.

A final certificate confirming compliance with the LR Code for UMS will be issued. An annexe to the certificate lists the key standards and items of evidence including the ConOps which now defines the operational limits and key assumptions. For novel technology, conditions may be imposed limiting operation or requiring operational experience to be recorded.

Finally, the completion of the process, results in a case for certification being made. These are currently being independently reviewed within LR to ensure that we can satisfy the questions raised in this paper and we are using the learning from this process to improve the assurance plans and initial workshops

It is important we establish the rigor of the safety argument with some key questions:

- Have the right questions been asked?
- Have the right people been included?
- Is the depth of assessment appropriate?
- Does the evidence base support compliance?
- Is the scope of certification clear?

They have not always been easy to answer, but we now have a good understanding of the end to end process and also what we expect to see in a unmanned systems design. Success in this means that LR can be recognised as having experience and expertise in this particular domain.

5 Conclusion

In recognition of the limitations in applying existing international codes, conventions and classification rules to unmanned maritime systems , Lloyd’s Register have developed a goal based Code for Unmanned Maritime Systems. This Code for UMS is written to cover all the safety aspects of the vessel and its control system. Operator competence, qualifications and management systems are not addressed. For environmental compliance it is recommended that MARPOL is followed.

The LR Code for UMS requires a systematic breakdown and assessment of the system at a level of detail sufficient to identify the hazards and risks within the system. Appropriate assurance activities are defined which will produce verification evidence and a robust safety assurance argument. The Code for UMS promotes a consistent and logical approach to the assessment of safety which will satisfy the requirements of regulators and other interested parties.

Key to the application of the code is the development of a concept of operations which allows the risks associated with UMS operation to be put into context and determines that the assurance provided is proportionate to the cost, size and risk profile of the vessels.

LR has been applying the Code for UMS to a number of unmanned systems under 24m, the majority of which are remote control or with constant supervision. From our application of the code we have identified two common issues which require a significant amount of justification. The first is the influence of people who launch recover, maintain and operate the UMS on the design requirements - managing the interface of people and machines are critical and need to be understood. The second is software which needs to be properly developed to appropriate standards to ensure safety critical and safety related functions are performed reliability. We also need to be careful to ensure duplicated and backup systems are diverse.

The LR Code for UMS is playing an important role, providing a framework for a safety argument and a format for discussions with regulator and other interested parties such as insurers. Assisting in the issue of exemptions and assessment of risk. It is being specified in some building contracts and to support some regulatory safety argument.

Some regulatory authorities have now recognised that application of the LR Code for UMS provides a documented and verifiable body of evidence that they can interrogate in order to support their own reviews. LR expects that this will continue to be the case going forward. Some regulators have already published guidance which recommends that the scope of the certification is agreed between LR and the Regulator at the start of a UMS project and informally recognising LR as a Recognised Organisation.

As the UMS industry evolves, and design solutions become more established the Code for UMS is expected to develop with it, to provide default prescriptive solutions such as those found in classification rules, whilst maintaining the goal based structure to ensure that it does not restrict innovation.

References

Lloyd’s Register 2017, Code for Unmanned Marine Systems. London. Lloyds Register.

Maritime UK 2021, Maritime Autonomous Surface Ships (MASS), UK Industry Conduct Principles and Code of Practice. London. Society of Maritime Industries.

INSA 2020, The Naval Ship Code, ANEP 77. Edition H Version 1. Brussels. North Atlantic Treaty Organisation.

IMO 1974, International Convention for the Safety of Life at Sea (SOLAS), as amended. London. International Maritime Organisation.

Paul James, Judith McKay, 2014. Goal based regulation – The NATO Naval Ship Code. 12th International Naval Engineering Conference and Exhibition May 2014. London. IMarEST.

H. Hoppe 2008. Goal-based standards – a new approach to the international regulation of ship construction. Maritime Safety Division, London. International Maritime Organization.

Lloyd's Register 2022. Rules and Regulations for the Classification of Naval Ships, London. Lloyds Register.

Lloyd's Register 2019. A Code of Practice for the Safety Assurance of Small Boats in Government Service. London. Lloyds Register.

Lloyd's Register 2022. Guidance Notes for Technology Qualification. London. Lloyds Register.

MCA 2004. Small Vessels in Commercial Use for Sport or Pleasure, Workboats and Pilot Boats – Alternative Construction Standards. London. Maritime and Coastguard Agency.

MCA 2021. The Workboat Code. The safety of small Workboats and Pilot Boats – A Code of Practice. Ed2 Am 1. London. Maritime and Coastguard Agency.

IMO 1978. International Convention for the Prevention of Pollution from Ships (MARPOL) as amended. London. International Maritime Organisation.

EU 2014. Pressure Equipment Directive. 2014/68/EU. Brussels. European Union.

Zhou 2017. Volvo admits its self-driving cars are confused by kangaroos . Guardian Newspaper.
Available from: https://www.google.com/amp/s/amp.theguardian.com/technology/2017/jul/01/volvo-admits-its-self-driving-cars-are-confused-by-kangaroos.

Glossary of Terms

ANEP	Allied Naval Engineering Publications
COLREGS	International Regulations for Preventing Collisions at Sea
CONOPS	Concept of Operations
IMO	International Maritime Organisation
ISM	International Safety Management Code
LOI	Level of Integrity
MAS	Marine Autonomous Systems
MASRWG	Marine Autonomous Systems Regulatory Working Group
MCA	Maritime and Coastguard Agency
SOLAS	Safety of Life at Sea Convention
STCW	Standards for Training and Certification of Watchkeepers
TRL	Technology Readiness Level
UMS	Unmanned Marine Systems