Guidelines on

Remotely Operated Vessels and Autonomous Surface Vessels

December 2021

IRCLASS
Indian Register of Shipping

Guidelines on

Remotely Operated Vessels and Autonomous Surface Vessels

December 2021

Contents

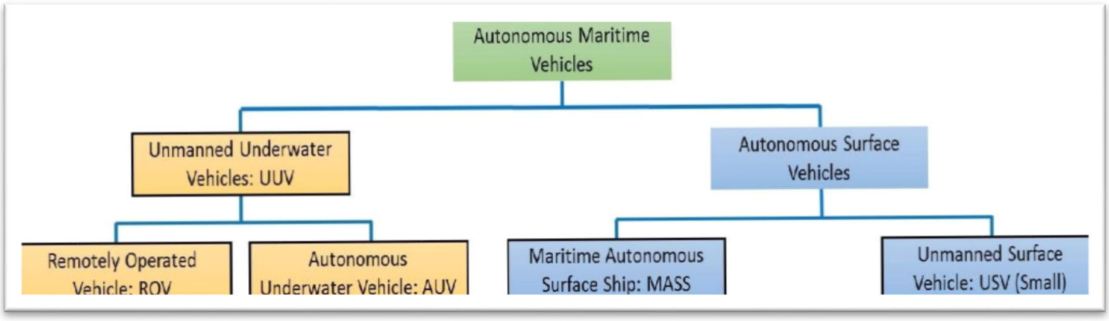
Sections

Introduction

The International Maritime Organization (IMO) took the first step to address regulatory aspects of autonomous ships in 2018. It used the term “Maritime Autonomous Surface Ship (MASS)” and defined it “as a ship which, to a varying degree, can operate independently of human interaction, and broadly laid out levels of autonomy.”

During the past few years different terminologies in addition to IMO MASS have been used for autonomous vessel especially surface vessels such as USV, ASV etc. In underwater technology, remote operated vessels (ROV) are already in use. It is therefore necessary to clearly understand the broad overall structure where all such vessels can be defined.

The figure below referenced from the “*Definition of autonomous ships*” by Norwegian forum of autonomous ships, indicates a broad overview of such vessels.



The focus of the present high level Guidelines is on Remotely Operated Vessels and Autonomous Surface Vessels with varying levels of autonomy.

The primary aim of this document therefore is to provide a broad framework (based on best practices), for the stakeholders involved in design, construction and testing of such vessels. The guidelines do not cover manning and operational aspects, which are to comply with the regulatory requirements, as applicable.

Section 1

General

1.1 Application

1.1.1 These guidelines are applicable to remotely operated vessels and autonomous surface vessels with varying levels of autonomy.

1.1.2 These guidelines are to be used in conjunction with other applicable Rules of IRS for construction and classification of vessels.

1.2 Goal

1.2.1 These guidelines are intended to provide requirements for safe and reliable operations of remotely operated vessels and autonomous surface vessels.

1.3 Functional requirements

1.3.1 The safety, reliability and dependability of the systems are to be equivalent to that which can be achieved with a comparable conventional vessel.

1.3.2 The probability and consequences of hazards are to be limited to a minimum through arrangement and system design.

1.3.3 The design philosophy is to ensure that risk reducing measures and safety actions are operated to minimize effect of loss of equipment or system.

1.3.4 The technical documentation is to be sufficient for an assessment of the compliance of the system and its components with the applicable rules, guidelines, design standards used and the principles related to safety, availability, maintainability and reliability.

1.3.5 System components are to be protected against external damages.

1.3.6 Safe access is to be provided for operation, inspection and maintenance.

1.3.7 Machinery, systems and components are to be designed, constructed, installed, operated, maintained and protected to ensure safe and reliable operation

1.3.8 A single failure in a technical system or component is not to lead to an unsafe or unreliable situation.

1.3.9 Suitable control, alarm, monitoring and shutdown systems are to be provided to ensure safe and reliable operation.

1.3.10 Fire detection, protection and extinction measures appropriate to the hazards concerned are to be provided.

1.3.11 Where vessel can be monitored and controlled from a remote control centre, safety of vessel and environment is to be ensured due to loss of vessel control arising out of failure of data communication link between vessel and remote control center

1.3.12 Commissioning, trials and maintenance of the systems are to satisfy the goal in terms of safety, availability and reliability and requirements of the flag Administration.

1.4 Definitions

1.4.1 *Automatic:* Pertaining to a process or device that, under specified conditions, functions without human intervention

1.4.2 *Autonomous Vessel:* Means that the vessel can perform operations for navigation or machinery control or both with reduced attention or no attention from the crew. This does not necessarily mean that no human is present. Such vessels plying on the surface are called Autonomous Surface Vessels (ASVs).

.

1.4.3 *Control position:* Means a location on the vessel during any periods of manned operation from which control of propulsion, steering and other systems can be exercised.

1.4.4 *Degrees of Autonomy*: The degrees of autonomy established by the International Maritime Organization in MSC.1/ Circ. 1638:

1.4.5 *Decision support system:* The system can perform information acquisition, information analysis and suggest actions to the operator to take decisions

1.4.6 *Essential systems:* Are that required to be operational for safety of vessel, personnel and environment. When the vessel is controlled or monitored from a remote location the systems at remote centre and communication systems also form part of essential system.

1.4.7 *Master:* For the purpose of these Guidelines, the term “Master” is to mean a specific person officially designated by the owner as discharging the responsibilities of the Master of the autonomous vessel. This person may be located anywhere provided that the required level of command, control and communication can be maintained to discharge responsibilities.

1.4.8 *Maritime Autonomous Surface Ship (MASS)*: As defined by the IMO, for the regulatory scoping exercise, MASS is a ship, which to a varying degree, can operate independent of human interaction.

1.4.9 *Unmanned:* means that there is no human present on the vessel bridge to perform or supervise operations. Crew may still be on board the vessel. Crew does not include passengers or special personnel.

1.4.10 *Remote Control:* Operational control of some or all operations or functions of vessel, at a point remote from the vessel.

1.4.11 *Remote Control Centre (RCC)*: A location external to vessel from where the vessel can be controlled.

1.4.12 *Unattended:* Means without a crew available to operate. In general, used for a control position, e.g. an unattended bridge, unattended engine room, etc.

1.5 Degrees of Autonomy

1.5.1 The degrees of autonomy specified by the IMO in MSC.1/Circ. 1638 are as follows:

Degree 1: *Ship with automated processes and decision support*

Seafarers are on board to operate and control shipboard systems and functions. Some operations may be automated and at times be unsupervised but with seafarers on board ready to take control.

Degree 2: *Remotely controlled ship with seafarers on board*

The ship is controlled and operated from another location. Seafarers are available on board to take control and to operate the shipboard systems and functions.

Degree 3: *Remotely controlled ship without seafarers on board*

The ship is controlled and operated from another location. There are no seafarers on board.

Degree 4: *Fully autonomous ship*

The operating system of the ship is able to make decisions and determine actions by itself.

Note: The above list does not represent a hierarchical order. It is to be noted that MASS could be operating at one or more degrees of autonomy during the duration of a single voyage.

1.6 Documentation

1.6.1 The following plans/ documentation are to be submitted to IRS, in addition to other applicable plans /documents as required for the type of vessel:

.1 *Concept Operational Philosophy (ConOp) document*: A ConOp document is to include vessel's role, operating area, operating profile, environmental limits along with maintenance and survey plans. The document is to also include details of various modes of autonomous operations and any other information as required by the flag Administration

.2 *Vessel functional specification document:* detailing following systems including roles and responsibilities.

- Machinery systems
- Navigation systems
- Communication systems
- Network and data flow
- Remote Control Centre
- Automation systems

.3 *Performance specification document:* describing the expected performance of the technology for certain defined parameters of automation

.4 *Vessel operational risk assessment document*: The document to indicate initial risk/ hazard analysis based on the functional description, Operation Design Domain, Dynamic Navigation Tasks and is to be prepared during concept design phase.

.5 *Vessel autonomous operation FMEA*: The document is to include a description of how a particular function behaves under different modes with regards to decision support, autonomy and remote control. The expected human interaction and the system behaviour is to be described including the system behaviour, if expected human input is not available in

- normal and emergency situations,
- network/ communication failure.

The document is to also include conditions which could result in degraded/limited functionality along with the consequences of the limitation(s). A description of the state(s) of the function in the event of a failure is to be specified.

.6 *Test and trial procedures*: This includes procedures for software, vessel systems, data storage during factory acceptance trials, harbour trials and sea trials

.7 *Data assurance document:* This document is to clearly identify data categorisation, data storage and data replay.

.8 *Cyber safety risk assessment*: This document is to contain details of assessment of cyber risks, vulnerabilities and mitigation measures. This is to be prepared at the concept design stage and reviewed subsequently as the design progresses.

Section 2

Design Philosophy

2.1 General

2.1.1 The ASV is to be designed and constructed to operate in all reasonably foreseeable operating conditions**.**

2.1.2 An autonomous vessel has some level of automation and self-governance. Automation is used as a general term for the processes, often computerized, that make the vessel able to perform certain operations without a human controlling it.

2.1.3 Autonomy is the result of applying "advanced" automation to a vessel so that it implements some form of self-governance, i.e. that it can select between alternative operating strategies without human intervention. A common autopilot, although being automatic does not provide autonomy by this definition as it always follows a given heading. Another example could be power management system is not considered as system with autonomy, which is programmed using a defined logic. The system does not have self-learning capability.

2.1.4 The emphasis is more on bridge automation as engines and other technical systems have already been extensively automated. Many vessels already have the capability to operate with periodically unmanned engine spaces. Navigation and bridge functions therefore form main focus for next generation development

2.1.5 The vessel is to be designed and operated to minimize the risk of fire and explosion including arrangement to minimize the spread of fire. It is to be possible to undertake maintenance and repair in accordance with the maintenance philosophy.

2.2 Operating design domain

2.2.1 The Operation Design Domain (ODD) is a definition of ship's operational area and constraints in which it has to operate. In effect ODD defines the environment in which the vessel is required to operate. The ODD is the basis on which necessary vessel functionality and its support systems are identified.

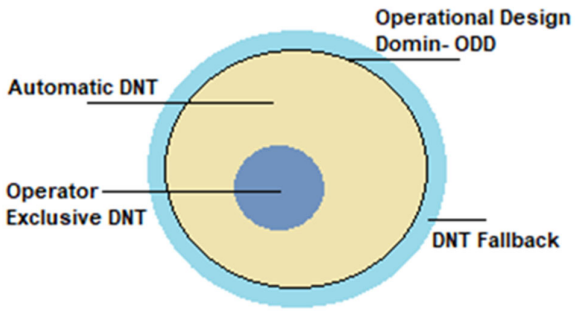


Fig. 2.2.1: Operation Design Domain

2.2.2The design is to include a systematic breakdown of various functions and identifying systems, sub systems and their interdependencies.

2.2.3 Dynamic Navigation Task (DNT) is a set of tactical operations supported to operate in a specified ODD.

2.2.4 The Operator exclusive DNT are set of tasks assigned exclusively to the operator. Typical example could be berthing, tug operations etc where the operator takes over the command

2.2.5 The Automatic DNT will be the set of tasks assigned to the automation system, This defines the requirements for sensor systems, object detection and classification, anti-collision systems etc.

2.2.6 DNT fallback is a predefined emergency procedure when ODD is exceeded. The DNT fallback should take the vessel to as safe a situation, as is possible under the given circumstances

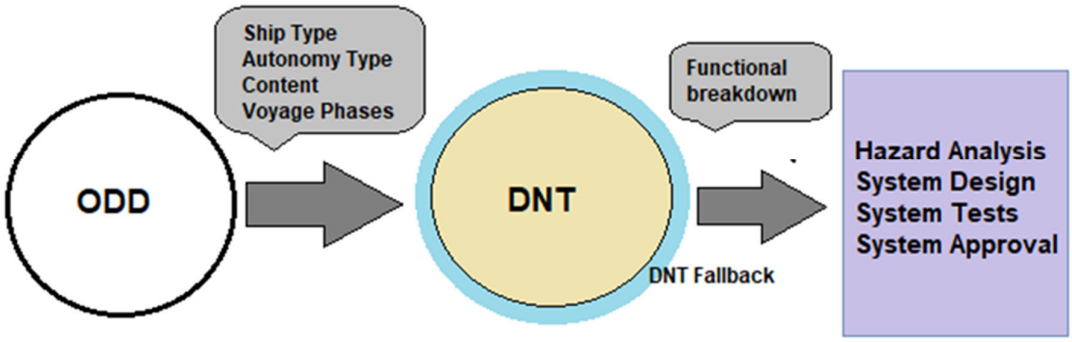


Fig. 2.2.5: Relation diagram for ODD, DNT

2.2.7 In accordance with the above, following steps are foreseen during conceptualization phase of an autonomous vessel:

- Define vessel ODD for the intended operation
- Define DNT and Fall back DNT considering various failure modes
- Define role and responsibility of human and system including decision making, control execution
- identify fall back options

2.3 Overview of Autonomous Systems

2.3.1 Essential process of autonomous vessel can be conceptualized as consisting of two basic integrated control systems a) Autonomous Machinery control system and b) Autonomous Navigation control systems. Both the control systems are integrated and controlled by Autonomous vessel controller

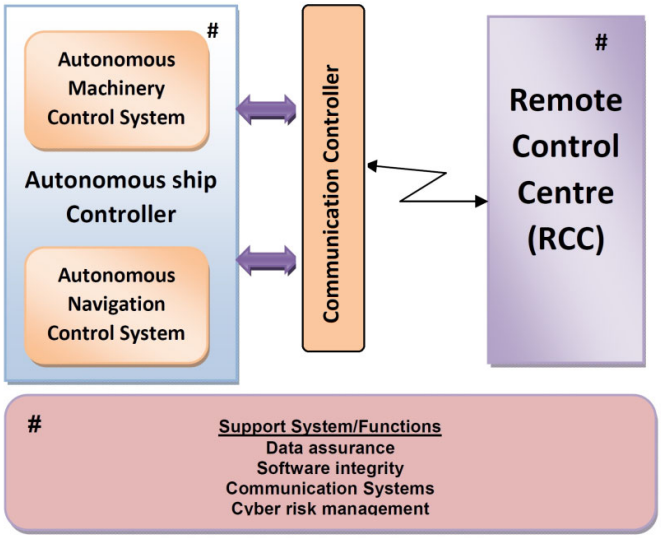


Fig. 2.3.1: Overview of Autonomous Systems

2.3.1.1 Autonomous machinery control system can consist of, but not be limited to the following:

- Engine control system
- Power management systems
- Computer based maintenance system
- Integrated machinery control system
- Emergency response

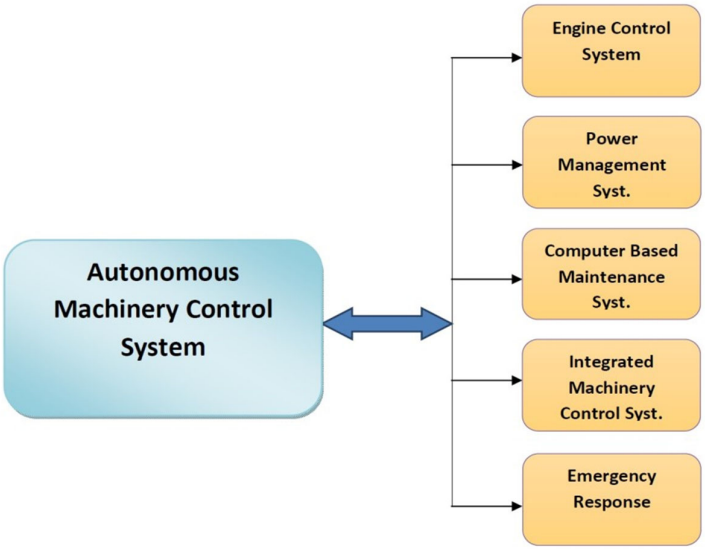


Fig. 2.3.1.1: Autonomous Machinery Control Systems

2.3.1.2 Autonomous navigation control system can consist of, but not be limited to the following:

- Situational awareness
- Voyage planning
- Collision avoidance
- Vessel control -speed and direction
- Equipment condition assessment
- Emergency response

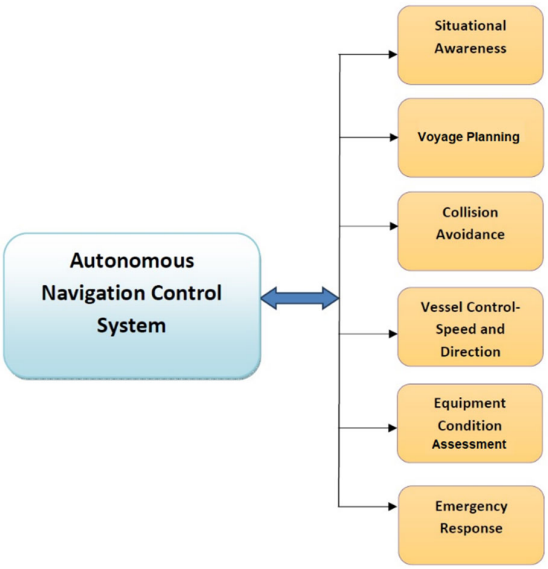


Fig. 2.3.1.2: Autonomous Navigation Control Systems

2.3.2 In an integrated computer based system, data flow, data creation, transfer and storage through software applications and data communication mode play a critical role in successful execution of intended operations. Following support systems/ functions are therefore considered critical and require attention from concept stage:

- Data assurance
- Software integrity
- Communication systems
- Cyber risk management

A vessel may have additional systems for cargo management docking/undocking etc. with varying degrees of autonomy levels

2.4 Decision making and execution

2.4.1 In a vessel with minimum automation, in general, the operator is required to perform the following functions:

- Situational awareness.is a three level process consisting of
    - *Perception*: Monitoring of various critical equipment;
    - *Comprehension* of the current situation; and

- *Projection* of future status of situation

- Decision making
- Control execution for implementing the decision

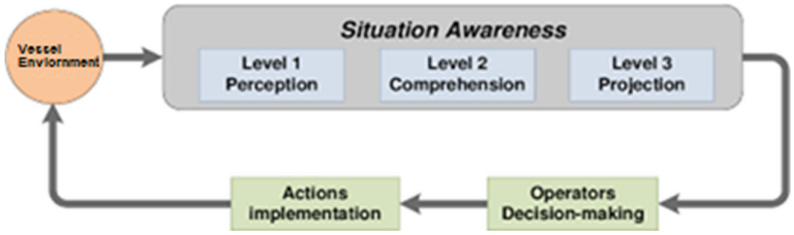


Fig. 2.4.1: Decision Making and Execution

2.5 Decision support tools

2.5.1 Decision support tool (DST) is a tool to assist the decision-maker. Such tools can broadly be categorized into two types Passive and Active

Passive decision support tool is a tool that aids the process of decision making, but that cannot bring out explicit decision suggestions or solutions.

Active decision support tool is a tool that brings out suggestions or solutions to support decision making.

For autonomous vessels the decision support tool as minimum is to be of the active decision support.

Note: Passive decision tools generally find their application in health monitoring systems for Machinery/ hull, vessel performance monitoring system etc.

2.6 Autonomy Levels and Certifications

2.6.1 Autonomous controls are aimed at gradual delegation of decision making and control execution functions normally carried out by the operator to a computer system. Accordingly for the purpose of these Guidelines, following autonomy levels are defined:

i. **AUTN 1** The system provides decision support for essential vessel systems. Decisions can be prognostic and system may present alternatives to operator. Decision making is by the operator who initiates control action after selecting the best alternative.

ii. **AUTN 2** The vessel is to have AUTN1 capability. In addition, its machinery and navigational systems can be remotely monitored and controlled.

iii. **AUTN 3** The vessel is to have AUTN 2 capability. In addition, it has the capability to select best alternative to initiate control action when permitted by the operator. Operator can intervene any time during operation *

iv. **AUTN 4** The vessel is to have AUTN 3 capability and additionally can initiate a control action and waits for predetermined time before executing the action. Operator can intervene before execution of action and also during emergency.

v. **AUTN 5** The vessel is to have AUTN 4 capability and additionally has the capability to select the best alternative and execute in autonomous mode. The Operator can intervene in emergency.

* Note: For vessels which can be controlled remotely, the system as minimum, is to have AUTN2 capability

vi. **AUTN-USV** A vessel less than or equal to 24 [m] operating in restricted or sheltered waters with no crew may be assigned notation AUTN-USV, when permitted by relevant flag Administration/ Statutory Authority and subject to meeting the technical requirements as per AUTN 2 level. Such vessels may be used solely for the purpose of defense /research/ short surveys. Such vessels are to have cellular or wireless network as back up for data communication. A statement of compliance will be issued by IRS to vessels complying with requirements for AUTN-USV when they are designed, constructed and tested solely for the purpose of technology demonstration.

2.7 Additional Qualifiers

2.7.1 As technology progresses the levels of autonomy also increase. There could be scenarios when only navigation and machinery systems are made autonomous instead of complete vessel. To facilitate such technological developments, additional qualifiers as below may be assigned for vessel with AUTN 1 level.

2.7.2 AUTN1 (N) may be assigned to a vessel if provided with navigation systems having decision support feature but with control execution feature under human control,

2.7.3 AUTN1 (M) may be assigned to a vessel if provided with machinery systems having decision support feature but with control execution feature under human control.

2.7.4 The suffix R will be added when the system can be controlled from location remote from the vessel. Ex AUTN 1-R(N)

2.7.5 The ODD will be included in the Class certificate /statement of compliance.

2.8 Vessels complying with the requirements of these Guidelines and having the Autonomy levels as defined above will be assigned class notations, as relevant and applicable, in addition to other notations required for Classification.

Section 3

Risk Assessment

3.1 General

3.1.1 The risk and technology assessment are required to be submitted for review at concept design stage.

3.1.2 The purpose of these assessments is to identify and to reduce risks due to hazards that may threaten the vessel within its operational limits. The aim is to reduce the risks to a level, As Low As Reasonably Practicable (ALARP)

3.1.3 The risk-based approach is to consider integrated onboard systems and systems onshore/ remote control centre.

3.2 Standards

3.2.1 The process for the risk assessment is to be based on techniques available in the following documents:

• ISO/IEC 31010 Risk management - Risk assessment techniques
• ISO/IEC 27005 Information technology - Security techniques - Information security risk management.

3.2.2 The risk assessment is to be performed at conceptual stage i.e. during formalisation of vessel model and is to be subsequently cross checked as the design progresses.

3.3 Methodology

3.3.1 The hazard identification is to cover all possible sources of hazards potentially contributing to undesirable events or accidents. The consideration of a functional failure associated with the consequence of an accident scenario is to govern the process of identification. As a guidance, a list of typical hazards for vessel are indicated below:

3.3.2 Risk Assessment is to consider ASV systems, sub-systems, and components, and following are to be taken in to account:

- The probability of a failure occurring, in measurable units, the direct and indirect effects of the failure;
- Whether the ASV is capable of inflicting significant damage in a collision
- Whether the ASV is liable to become a significant obstruction to other traffic, if left to drift without propulsion or steering. This is governed by size and weight and operating area.
- Whether the ASV carries significant quantities of hazardous or pollutant substances.

3.3.3 Risk Assessment is to be performed to identify potential failures such as grounding due to collision with a fixed or a floating object

- Grounding
- Fire
- Stability
- Pollution, such as leakage of harmful substances etc. due to fire, collision, grounding

- Failure of Communication equipment and signal links,
- Breakdown of Electrical power, sensor and IT system,
- Failure of Cyber security (data communication breach, spoofing, etc.),
- Inconsistency of data and failure in automated decision-making,
- Becoming an obstacle to navigation of other vessels due to Machine, power, steering or propulsion breakdown

3.3.4 Systems to be considered in the Risk Assessment are as follows

- Power generation, control, distribution;
- Propulsion systems including the control of thrust and its direction;
- Steering systems including actuators and their control;
- Fuel and hydraulic systems
- Sensors and actuators;
- Navigation and communication systems;
- Situational; awareness system
- The autonomy processor(s), i.e. the interpretation and decision-making system which takes in sensor data and takes decisions on what control actions to take. This may be done on board, off-board, or as a combination of these;

3.3.5 The Risk Assessment is to show that the vessel can be operated at a tolerably safe level, ideally proven to be as safe as an equivalent manned counterpart (i.e. similar size and carrying similar payload).

Section 4

System Requirements

4.1 General

4.1.1 This section details the system requirements recommended for vessels using advanced automation and varying degrees of autonomy. The extent of redundancy, technical design and backups increase with autonomy level, type of vessel, intended operation of the vessel and area of operation. The designer is to submit all the relevant details indicating compliance with the functional requirements specified in this Section and Section 2 of these Guidelines.

4.1.2 The systems are to be designed to operate in all reasonably foreseeable operating conditions and are to meet requirements for watertight, weathertight and fire integrity. The design is to be aimed at minimizing the risk of initiating fire and explosion. The design and arrangement of equipment is enable the maintenance.

4.2 Hull

4.2.1 The structure is to be designed, constructed and maintained with a level of integrity sufficient to enable the ASV to be operated and maintained safely as and when required within its design or imposed limitations.

4.2.2 The buoyancy, stability, watertight and weather tight integrity are to be sufficient to enable the ASV to be operated safely.

4.2.3. Any penetrations in the structure of the ASV are not to affect the watertight and weather tight boundaries.

4.2.4 The vessel is to be designed and operated to minimize the risk of initiating fire and explosion including arrangement to minimize the spread of fire.

4.2.5 It is to be possible to undertake maintenance and repair in accordance with the maintenance philosophy

4.3 Machinery and Electrical Systems

4.3.1 Machinery system

4.3.1.1 The machinery system is to be suitable for unattended operation and in general all essential and safety machinery systems including maintenance are to be designed with the above philosophy. The machinery system is to be designed to minimize the risk of fire,

4.3.1.2 The maintenance system is to provide a systematic monitoring, analysis and prediction of equipment health to minimize down time.

4.3.1.3 Emergency situations as identified through risk analysis are to be handled by the system.

4.3.1.4 The auxiliary systems are to be designed to support mission functions.

4.3.1.5 The ASV is to have a defined emergency stop condition, which is to be fail safe under conditions where normal control of the ASV is lost. Under Emergency Stop, propulsion is to be reduced to a safe level in a timely manner. A safe level could be defined as a level at which it is not likely to cause damage either directly or indirectly. The phrase *"in a timely manner"* means within a time that is short enough to ensure that the risk from uncontrolled propulsive power can be contained before it is likely to cause damage in open ocean conditions. Various conditions/ scenarios which would necessitate activation of

emergency stop are to be identified and documented.

4.3.1.6 The philosophy of fail to safe is to be as per applicable Rules and specific to notation. Alerts and indications are to be provided as per rules at local, bridge and remote control centre.

4.3.1.7 Fire safety systems are to be designed to detect and extinguish a fire with a level of integrity sufficient to enable the ASV to be operated and maintained safely and to protect the vessel in al designed operating environment

4.3.2 Electrical and control system

4.3.2.1 The vessel is to be provided with one centralized controller hereinafter referred as autonomous machinery control system to control all machinery systems required for propulsion and safety, including auxiliary systems. The autonomous machinery controller is to be provided with dual controller. It is to be possible to monitor and control all systems required for propulsion, manoeuvring and safety of the vessel from local, bridge and where required from remote control centre. Control system redundancy for controllers, networks and power supply is to be provided as per the applicable notation and risk analysis,

4.3.2.2 The autonomous machinery control system is to be interfaced with autonomous navigation control system for vessel with autonomy level AUTN 2 and above.

4.3.2.3 Additional sensors such as CCTV cameras, infra-red cameras, water ingress etc. are to be installed to detect vessel safety critical situations and to deploy suitable countermeasures to mitigate the risks. The extent of automation and sensors is to be sufficient for the intended vessel autonomy level.

4.3.2.4 The electrical system is to be designed with a level of integrity sufficient to enable the ASV to be operated and maintained safely.

4.3.2.5 Sufficient electrical power is to be provided to supply the required services of the ASV during all identified vessel operational modes, The power supply system is to be designed to supply, for the ASV to conduct its mission with an appropriate level of redundancy, The location, arrangement and operation of the electrical power system is to be according to requirements for an unattended machinery space.

4.3.2.6 An independent emergency source of power, located as per SOLAS is to be provided and is to have sufficient capacity to power emergency loads as per SOLAS and additionally for critical systems as identified in the risk analysis.

4.3.2.7 Automation and extent of autonomy are to be in accordance with concept design philosophy and the extent of redundancy required for a particular system as identified through risk analysis. Restoration of key process/ functions though automatic operation of redundant systems are to be the normal philosophy

4.3.2.8 Suitable arrangements for the safe installation, use and maintenance of energy storage devices are to be provided.

4.3.2.9 Machinery, electrical and safety systems as required by applicable Rules are to be provided

4.3.2.10 Independent of autonomy level, provision for local /emergency back up control is be provided.

4.3.2.11 Transfer of control is to be defined and documented. Transfer of control in case of loss of communication or system is to be defined at design phase and submitted for approval.

4.4 Navigation and Communication Systems

4.4.1 The system is to be designed for integrated bridge operation to achieve objective of smooth navigation of the vessel using decision support systems.

4.4.2 The system is to consider changing environment, vessel dynamics, buoyancy and stability and avoid collisions while navigating the vessel.

4.4.3 The system is to be interfaced with autonomous machinery control system for vessel with Notation AUTN2 or higher.

4.4.4 The changing environment within and outside the vessel is to be monitored on real time basis and analyzed. Where a computer based system plays a critical role for above function, the system is to be designed as per relevant Rules. The systems are to advise/ act on a developing situation to avoid dangerous situations such as collision, grounding.

4.4.5 The systems are to be interfaced with the emergency response system as appropriate for the autonomy level and vessel operational profile.

4.4.6 Internal and external communication systems are to comply with the requirements of the requirements of the flag Administration.

4.4.7 All statutory requirements applicable for the type of vessel are to be complied with.

4.4.8 The bridge equipment is to be designed with Bridge Alert management system

4.4.9 It is to be possible to send all reports as required by relevant administration including VTS stations.

4.4.10 Equipment is to be designed with built in test feature

4.4.11 The vessel is to have the feature to update the route information to remote control centre (when provided). The remote control center also is to be provided with facility for voyage planning. Responsibility of plan updating is to be clearly defined. The remote control centre is to be provided with weather and other navigational data towards above.

4.4.12 The data communication link is to be designed for transfer of raw video data or target information as per vessel ODD and risk analysis.

4.4.13 Docking and undocking operations are to be in general are to be carried by operator. Novel designs can be approved specific to project. In such cases, detailed risk analysis is to be submitted for such operation.

4.4.14 COLREGs and other statutory requirements are to be complied with, requirements of the flag Administration. All the equipment for AUTN 2 and above are to be provided with feature for remote monitoring and control.

4.4.15 Sufficient documentation /operational manuals are to be provided on board and where required at remote control centre on operation and maintenance

4.4.16 The safety and efficiency of navigation by improved provision of position, navigation and timing (PNT) data to bridge teams and remote centre and shipboard applications (e.g. AIS, ECDIS, etc.) are to be in accordance with relevant IMO requirements and are to be provided with feature for remote monitoring and control. (for AUTN 2 and above)

4.4.17 The vessel is to be provided with a feature with backup communication which is to be sufficient to transfer the safety critical data to shore centre in the event of loss of main communication link. Transfer from main communication link to backup is to be smooth and automatic. The bandwidth and latency requirements are to meet the designed system philosophy.

4.5 Situational Awareness and Control

4.5.1 A situational awareness and control system for the ASV can include on-board sensors and off-board information sources (Audio and Visual), communications links and control logic which together ensure safe operations.

4.5.2 The situational awareness and control are to ensure that the ASV, and RCC when appropriate, have sufficient information, interpretation and control of its position and systems, to enable it to be as safe as a manned vessel operating in similar circumstances.

4.5.3 Any decision making that impacts safety and is performed by the ASV (i.e. independent of a human operator) is to be adequately demonstrated to be commensurate with that, which a competent seafarer would correctly perform in the same situation.

4.5.4 A Risk Assessment is to be undertaken using an appropriate method, e.g. Failure Mode Effects Analysis (FMEA), in order to identify the risk levels associated with the ASV and its operation. The analysis is to be supported by appropriate trials.

4.5.5 Internal and external sensors may be used to monitor the state of the platform and the external environment.

4.5.6 It is necessary to have the ability to interpret sensor data in terms of its immediate or impending impact on ASV performance, and its direct or indirect effect on the safety of the ASV, surrounding structures and vessels, humans and the environment.

4.5.7 Operators are to be provided with adequate access, information and instructions for the safe operation and maintenance of the control system.

4.5.8 The number, type and location of the sensors are to be vessel specific and are to be selected as considered essential so as to ensure the necessary levels of safety equivalent to a manned Vessel.

4.5.9 The overall need for monitoring is to depend on the considerations above, being guided specifically by the outcome of the Risk Assessment.

4.5.10 The sensor systems are to maintain an automatic lookout for traffic and obstacles as well as lookout for environmental conditions surrounding the vessel. The overall goal of the sensor module system is to maintain lookout by all available means so that an unmanned vessel can comply with basic functionalities as required by COLREGs, minimize the risk of collision and ensure safe voyage. The system may employ and advanced integrated sensor fusion technology to overcome limitations of individual sensors. The data/information from various sensors are fused which would aid in decision support system.

4.5.11 *External environment monitoring sensors*: External sensors are to be installed at appropriate locations to sense and/ or measure the environment, surroundings, navigational data, and other information which may include, but not be limited to, the following:

- Heading
- GNSS(Lat/Long);
- Sea state
- Wind speed and direction;
- Depth
- Raw radar video and extracted radar targets;
- Sound signals;
- Visual signals, such as shapes, carried by other vessels or navigational marks;
- Situation awareness near to vessel through state of the art low range radars and high definition CCTV systems which could help in identifying small floating objects

The exact number and performance requirements for, the sensors will be dependent on the ASV operational profile, level of control required and are to be ascertained through the Risk Assessment.

4.5.12 *Internal vessel monitoring sensors*: Internal sensors may be fitted for monitoring the platform's vital functions and safety. In addition to alarms and indications as required for periodically unmanned spaces, monitoring capability for different functions is to be provided which would normally be carried out by crew onboard. A few examples of such sensors are as follows:

- Health status of command data links, in particular those with the ability to receive an Emergency Stop command (essential);
- Operability and health status of sensors that are identified as vital;
- Operability and health status of on-board systems such as propulsions, platform control systems, collision avoidance systems, autopilots, servos, communications data links, and other internal sensors which may be needed to maintain platform and mission integrity;
- Onboard audio facilities:
- Remaining fuel;
- Watertight Integrity of the hull (or hulls);
- Structural damage to the overall ASV or its components;
- Pitch, roll and heave;
- Vibration;
- Shock;
- Payload integrity / fuel leaks: greater need;
- Endurance;
- Outside Line of Sight, greater need for monitoring;
- Level of Control (See definition at 1.4.7);
- Appropriate monitoring required for the level of control in operation

4.6 Network Architecture

4.6.1 As the autonomy level increases, the integration of computer based system increases, making the network architecture inside a vessel an important function to be addressed in autonomous vessel. Network architecture is to be carefully designed either for smooth data flow between the systems inside a vessel or between vessel and remote control center,

4.6.2 Networks for safety critical systems and integrated systems are to be resilient. The design is to be such that in the event of a fault in one part of the vessel network due to failure of network devices or cyber incident, the remaining systems connected to unaffected network are adequate to allow the vessel to continue its mission-critical operations in a manner that preserves the confidentiality, integrity, and availability of the data necessary for the safety of the vessel.

4.6.3 Network communication documents are to be used for specifying means of communication between various sub systems and various components of sub system.

4.6.4 The criterion for communication network design is to be based on the following:

- Reliability;
- Maintainability;
- Extensibility;
- Interoperability.

4.6.5 Suitable methods/arrangements are to be considered during design phase to improve the network resilience. Towards above, network segregation and definition of appropriate levels of privileges, need careful consideration during concept phase.

4.6.7 Network devices

4.6.7.1 Network devices are to comply with the following:

a) Network devices, monitoring and alarm devices for Category II and III systems are to be suitable for marine application and are to be tested as specified in Part 4, Chapter 7, Section 6 of IRS *Rules and Regulations for the Construction and Classification of Steel Ships* and IRS Classification Note: *Type Approval of Electrical Equipment used for Control, Monitoring, Alarm and Protection Systems for use in Ships* or other relevant standards which are acceptable to IRS

b) All network cables for Categories I,II, III systems are to be designed, manufactured and tested as per relevant national/international standards acceptable to IRS .

c) Suitable network monitoring and alarm systems are to be deployed. The network monitoring systems is to provide adequate information describing the cyber incident for the use of the intended user. When the vessel has provision for remote connectivity it is to be possible to identify a cyber-incident originating external to vessel.

4.6.8 Network redundancy

4.6.8.1 Network design is to be based on risk assessment and the system philosophy. Data sizing calculations are an important aspect in network design, both in terms of speed and throughput. Towards data sizing following factors are to be kept in mind to identify suitable network:

Data throughput
- Data Speed requirement for particular application;
- Data format.

Data categorization, data classification, data format and data content is to be as per international standards such as IEC 61162 or other equivalent standards.

4.6.9 Network Control, Monitoring and Alarm

a) Monitoring

Network devices are to be able to detect following states by performing self-diagnostics:

i. Link up of each port on the network device
ii. Link down of each port on the network device
iii. Power on or hardware reset
iv. Network storm detection
v. Fan failure (only if the network device has a fan and a fan-stop detection function)
vi. Abnormal temperature (only if the network device has an abnormal-temperature detection function.

b) Alarm function

The network-monitoring device is to provide functions to detect abnormal condition and notify the user:

i. When a link is disconnected or the power is turned off for a network device or network terminal
ii. When a link not belonging to the network is connected or the power is turned on for a network device or network terminal
iii. Loss of a network device.

4.6.10 Wireless Communication

4.6.10.1 The access control system is to provide capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.

4.6.10.2 The access control system is to provide capability to authorize, monitor and enforce usage restrictions for wireless connectivity to the control system according to commonly acceptable industry best practices.

4.6.10.3 The wireless access point is to provide capability to employ encryption mechanisms to prevent loss of integrity and confidentiality of information during communication.

4.6.10.4 Wireless equipment is to be designed and tested as per requirements specified in Part 4, Chapter 7, Section 6 of IRS *Rules and Regulations for the Construction and Classification of Steel Ships*.

4.6.11 Network protection safeguards

4.6.11.1 Suitable network protection and detection systems, based on network criticality analysis are to be provided for inter network communication. Following controls are to be provided:

i. Management of identities and credentials of network users, including M2M networks
ii. Enhanced authentication control, or restricted privileges, for remote access or from access points of the lower level of security
iii. Physical access control to network access points
iv. Pervasive implementation of Least Privilege Policy
v. Encryption for data at rest (stored) and data in transit (exchanged)
vi. Integrity checks for data at rest and data in transit
vii. Separation of networks, firewalling, De-Militarized Zones (DMZs), etc.
viii. Separation of networks supporting IT systems (e.g. for administrative tasks, passenger and crew connectivity, etc.), OT systems (e.g. for engine control, cargo control, etc.) and alarm systems
ix. Event logging and Quality of Service (Quos)
x. Use of routing technology for vessel to shore and vessel to vessel communication, Where considered necessary through risk assessment, separation of CAT I ,CAT II, CAT III systems networks is to be implemented.
xi. Where considered necessary through risk assessment additional layers of controls is to be provided(A defense in depth approach).

4.6.12 Installation of any software in integrated systems (during integration phase onboard) is to be carried out through the usage of controlled computer, removable media or DMZ. Direct connection to the internet is to be avoided.

4.6.13 Suitable network protection and detection systems, based on network criticality analysis are to be provided for inter network communication. Suitable network protection devices at perimeter level or between networks are to be provided.

4.6.14 Standard interfaces are to be used for data exchange between different networks. Each network is to be designed in compliance with recognized international standards such as IEC 61158 or IEC 61784, etc. or equivalent.

4.7 Cyber Resilience

4.7.1 Cyber-attacks on a vessel's critical OT Systems, IT and navigational systems, can result in physical loss of vessel or damage, loss of cargo, loss of reputation, loss of business data, crew personnel information and environmental damage. The aim is to deliver cyber resilient vessels, whose resilience can be maintained throughout their service life.

4.7.2 Resilience, in this context, is meant as a characteristic that provides crew and vessel the capabilities to effectively cope with cyber incidents occurring on computer-based systems onboard which contribute to operate and maintain the vessel in a safe condition. The most effective method of dealing with an incident is to prevent it ever happening, so in this context "prevention" is even more important than "cure".

4.7.3 It is to be ensured that design, integration and/or maintenance of computer-based systems support secure operation and provide means to protect against unauthorized access, misuse, modification, destruction or improper disclosure of the information generated, archived or used in onboard computer-based systems or transported in the networks connecting such systems

4.7.4. For a conventional vessel with normal manning, the risks mitigation measures are always a combination of technical, managerial and operational procedures. However as the autonomy levels increase the technical controls play a major role especially for cyber security protection of onboard systems.

4.7.5 Data transmission to computer based systems on board of category II and III, which is critical for the safety of navigation, power and cargo management, is to be protected against unauthorized access and is to have the necessary capabilities to mitigate the risks arising due to remote access. The equipment is to have the capability to terminate a connection from the onboard terminal and revert to the known and uncorrupted state. Where equipment does not have the capability, the same is to be arranged through installation of additional network devices, which support such functions.

4.7.5 In the event of a cyber-incident, the system is to ensure that, locally it is possible to restore to a situation delivering a full and safe local access to the operations. The risk assessment is to take into account threats and mitigation measures associated with remote access.

4.7.6 Systems/equipment is to have capabilities necessary to prevent interruptions to remote access sessions interfering with the integrity and availability of OT or the data used by OT systems.

4.7.7 A test plan is to be developed to test the satisfactory functioning of remote access feature. The test program is to be prepared and executed by the Supplier or System Integrator The test program is to include procedures for functional tests and failure tests. Relevant results/ observations are to be recorded in a test report

4.7.8 Configuration of network devices

4.7.8.1 Networks, that are provided with remote access are to be controlled (i.e. designed to prevent any security risks from connected devices by use of firewalls, routers and switches (reference IEC 61162-460:2018 + Amd1:2020) External access of such connections is to be secured to prevent unauthorized access.

4.7.8.2 Network devices, such as switches are to be provided with configuration parameters, such as

i. Password encryption
ii. Password protected console ports
iii. Configurable session timeouts
iv. Flow control enabled
v. Unused ports closed

4.7.9 When it is intended to control critical vessel functions from remote control centre, the onboard computer systems are to meet the requirements for class notation **CyS-II** as specified in IRS *Guidelines on Maritime Cyber Safety*

4.7.10 The shore/ remote control centre facilities are to be assessed for Cyber Safety based on IRS *Guidelines on Cyber Safety of Land Installations* (shore based systems). IACS Recommendation I66 and requirements of CYS II+ notation in the subject IRS Guidelines may also be referred.

4.7.11 The computer based systems are to be designed and tested for Level 4 security level as per IRS Classification Note: *Type approval of Cyber Secured Control System Components*.

4.7.12 Cyber Incident Response measures

4.7.12.1 The System Integrator and Supplier is to consider and implement measures aimed to take appropriate actions regarding detected cyber security events on networks so as to limit the cyber incident impact to the network zone of origin. The measures are to be aimed to minimize the possibility of disruptions to OT systems, which could have effect on availability of systems required for safety critical functions. The measures along with test plan are to be developed

4.7.13 Following advanced security measures as applicable are to be implemented on board (especially where IT systems are integrated with OT systems) and is to be based on risk analysis specific to an installation:

i. Virtual private network (VPN) is to be deployed into the network. VPN protocols are to encrypt traffic going from sender to receiver.
ii. Intrusion prevention system (IPS) is to be deployed into the network. IPS is to issue an alarm in case of starting to record events that may affect security. It is to also block unwanted traffic.
iii. Alarm from IPS is to be generated at the relevant and centralized station which is normally considered to be manned.
iv. IPS is to contain predefined signatures (database of attack signatures), custom signature entries, out-of-band mode, packet logging.
v. Data loss prevention (DLP) software is to be implemented to prevent “leakage’’ of important data.
vi. Content filtering technology module is to be installed. This device is to block traffic to and from a network by IP address, domain name/URL and type of content.
vii. Anti-spam filtering is to be applied.

4.8 Data assurance

4.8.1 The data assurance assessment is required to establish and mitigate the risks of identified data properties so that the system operates in a safe manner. There are various data property types which are to be identified. Safety-related data that contribute to, are used by, produced by or affected by business critical, essential services or safety critical systems are to be ascertained.

4.8.2 Data Security

4.8.2.1 The general objective of data security are to ensure the confidentiality, integrity and availability of Data. Depending upon the intended use of the data, these may take a different order of priority. For example, OT systems transmitting safety critical data will prioritize availability and then integrity. The three terms can be broadly defined as below.

Confidentiality – a loss of confidentiality is the unauthorized disclosure of information.
Integrity –a loss of integrity is the unauthorized modification or destruction of information.
Availability – a loss of availability is the disruption of access to, or use of an information system

4.8.2.2 The scope of application of Data Assurance covers data whose lifecycle is entirely within on board computer based system, as well as data exchanged with shore systems connected to the on board networks. While the consequences of un-authorised modification, data corruption or data loss may differ between IT systems data (typically operational data with a business impact) and OT systems data (may include set points for machinery control and safety with a safety or environmental impact), where data transfers and updates are implemented using a network, these data security objectives share common features and are to be considered for the system as a whole.

4.8.3 Data Categorization

A data categorization document identifying the risks for various categories of data is to be developed.

4.8.3.1 Data is to be categorized by the supplier or system integrator according to the possible consequences of a breach of data assurance on the three security objectives confidentiality, integrity and availability

4.8.3.2 The potential impact of loss of data assurance is to be categorized as follows:

LOW: The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on human safety, safety of the vessel and / or threat to the environment.

MODERATE: The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on human safety, safety of the vessel and / or threat to the environment.

HIGH: The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on human safety, safety of the vessel and / or threat to the environment.

The following table (Table 1) shows how to assign system with categories based on their effects on system confidentiality, integrity and availability.

Table 1: System Categories and Effects					
Category	Effects	System functionality	Confidentiality	Integrity	Availability
I	Those systems, failure of which will not lead to dangerous situations for human safety, safety of the vessel and / or threat to the environment.	Monitoring function for informational / administrative tasks	Low	Moderate	Low
II	Those systems, failure of which could eventually lead to dangerous situations for human safety, safety of the vessel and / or threat to the environment.	Alarm and monitoring functions Control functions which are necessary to maintain the vessel in its normal operational and habitable conditions	Moderate	High	Moderate
III	Those systems, failure of which could immediately lead to dangerous situations for human safety, safety of the vessel and / or threat to the environment.	Control functions for maintaining the vessel's propulsion and steering Safety functions	Moderate	High	High

4.8.3.3 The categorization described above is to be used as guidance and definitions are to be assessed on a case by case basis.

Note 1. *Escalation*: systems involving essential services sharing data necessary for their functions might need to have the potential impact escalated to a higher level.

Note 2. *Confidentiality level*: it is understood the confidentiality level of information might have an immediate business risk.

4.8.3.4 Data properties are to establish what aspects of the data (e.g., timeliness, accuracy) need to be guaranteed in order that the system operates in a safe manner.

4.8.3.5 An analysis is to be carried out by the system integrator to assess the value of data security and its potential impact on system performance.

4.8.3.6 Devices used to store data for category II or III systems are to be appropriate for intended use and suitable for the marine environment. Data stored on such devices is to be appropriately replicated to minimize data loss in case of device single failure.

4.9 Software Assurance

4.9.1 Design, development and testing of software is to be carried out in a structured manner by following well laid procedures /standards to ensure reliable operation of software. The software is to be designed and tested in accordance with IRS *Guidelines on Certification of Software for Computer Based Control Systems*. These Guidelines help to reduce the software related incidents, which if not addressed can affect the safety of the vessel. These Guidelines are applicable to standalone or integrated computer-based systems

4.9.2 A global top to bottom approach is to be undertaken regarding software and the integration in a system, spanning the software lifecycle. The validation and verification approach for the software is to be accomplished according to software development standards indicated in Part 4, Chapter 7, Section 6 of IRS *Rules and Regulations for the Construction and Classification of Steel Ships*, or equivalent standards acceptable to IRS.

4.9.3 Logical security measures such as authorization and authentication procedures are to be in place to prevent unauthorized or unintentional modification of software, whether undertaken at the physical system or remotely

4.9.4 When a software revision can lead to hardware change, the hardware used is to be suitable for the equipment or system according to applicable requirements of IRS.

4.9.5 The backup and recovery of software and data is to be considered in design phase

4.9.6 Development of testing of decision support systems machine learning and artificial intelligent systems are to be discussed in details before the commencement of the project, The standard test cases and verification at module level are to be agreed upon As the output of Machine Learning and Artificial Intelligence systems is based on self-learning ability of the software, the methodology, test cases and tests data base requirements are to be submitted to IRS prior to project initiation. The reparability of the systems for similar operating conditions and inputs will be required to be verified extensively especially for systems which are self-learning. Loss of inputs which could result in unexpected system hanging are to be analysed

Section 5

Remote Control Centre

5.1 General

5.1.1 An ASV when intended to be controlled and/ or monitored from a location remote from vessel should be provided with a Remote Control Centre (RCC). The centre may control and monitor single or multiple ASVs.

5.1.2 The RCC may be located a on a separate vessel or at shore. The RCC may also interface with other RCCs that are separately located. Risk assessment is to be carried out while formulating the responsibilities and division of responsibilities at RCC and the vessel.

5.1.3 The RCC architecture may vary from system to system and could be location specific. However following tasks are to be undertaken to a level appropriate for the mission, in accordance with the risk assessment:

5.2 Design Philosophy

5.2.1 The remote control centre design is to be based on following key aspects

- **Survivability** – A single failure in the system will not interrupt the control and monitoring function of RCC.
- **Redundancy** – Vital monitoring and control functions remain operational and operating at RCC when the vessel system is exposed to adverse conditions
- **Modularity** -Hardware and software of RCC is to be modular by design for scalability, best maintainability, and operational flexibility.
- **Reliability** – Hardware and software components of the RCC systems are to be proven for applications under different operating conditions, noting that malfunctioning of hardware and/ or software may lead to accidents.
- **Maintainability-** Systems in RCC are to be easy to maintain without disturbing operation of vessel at sea. Data backup is to be considered for restoring systems after maintenance

5.2.2 It is to be possible to observe real-time operational status, readiness and capacity of the vessel function or system from the centre

5.2.3 Abnormal conditions and situations are to generate alerts that, in general, are categorised and prioritized in accordance with the principles of IMO Resolution MSC. 302(87) *Performance Standards for Bridge Alert Management* and IMO Resolution A.1021(26) *Code on Alerts and Indicators*.

5.2.4 The responsibility of responding to an alert should be defined in accordance with vessel autonomy type. A operation philosophy document is to be developed clearly specifying the roles and responsibilities of remote control centre including manual responses, transfer of control, primary and secondary control locations and handling of emergency situations.

5.2.5 The system is to be designed with dual state authentication systems. Only one location (on board/ RCC) is to have the privilege for control of a vessel function or an equipment at any time. It is to be possible to override or perform emergency control on board the vessel.

5.2.6 The RCC is to be provided with necessary hardware and application software for carrying out its intended operations.

5.2.7 The RCC can be designed for two operating modes:

1. Remote monitoring and decision support of vessel with crew onboard.
2. Remote monitoring and control of vessel with/without crew onboard. (As permitted by the flag Administration)

In the first mode, all vessel parameters will be monitored and analysed from RCC and it will provide necessary support to vessel operator for decision making during vessel operation. In the second mode, all vessel parameters will be monitored from RCC and it can control the vessel operation.

5.2.8 Transfer of Controls

5.2.8.1 The vessel bridge is considered as the primary operation centre and controls can be transferred from the vessel to RCC.

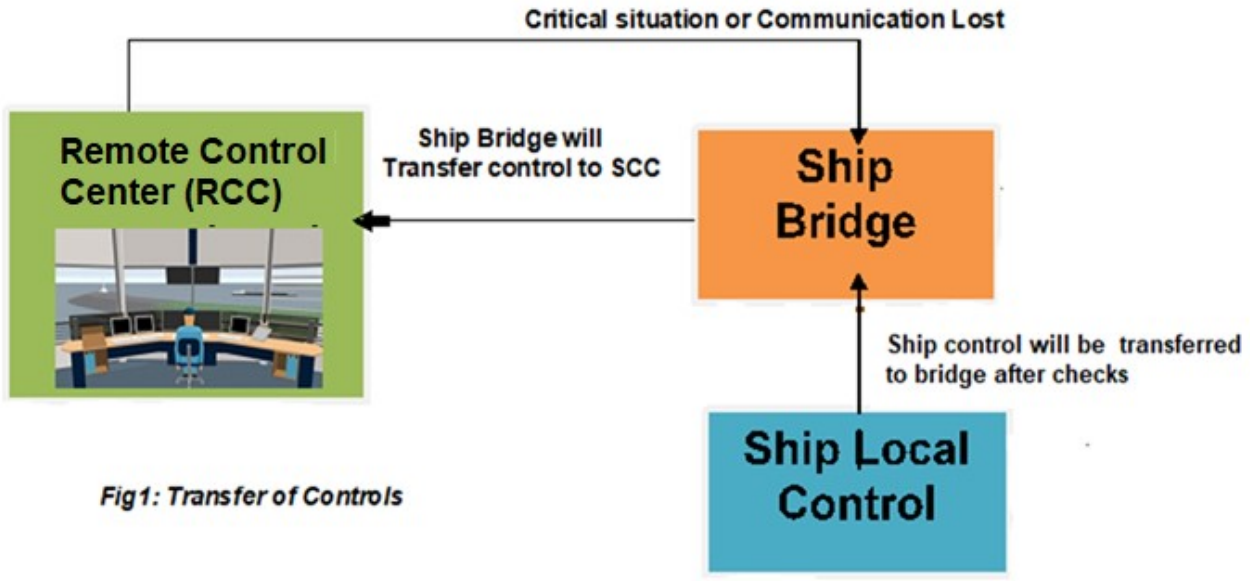


Fig1: Transfer of Controls

Fig. 5.2.8.1: Transfer of control from Vessel to RCC and Vice Versa

5.2.8.2 The order of transfer of control is to be from vessel to remote control centre. Control is to be automatically transferred back to vessel bridge in case of loss of communication or any other critical situations. Such situations should be defined in the operation philosophy documents, based on risk assessment.

5.2.8.3 Basic functions of the RCC are as follows:

- Situation awareness and Decision Support
- Control and Monitoring of vessel systems including navigation
- Alarm Handling
- Communication (With nearby vessels, Port, Third party supplier)
- Remote Training for installation, Maintenance and Trouble shooting.

5.3 Remote Control Centre Layout

5.3.1 Work stations in the RCC are to be ergonomically designed and are to be provided with high-resolution colour monitors that display graphical pages of the machinery and systems, as appropriate. Each work station is to be provided with appropriate password authorization and the control transfer protocols are to be complied with. Display and controller redundancy are to be provided for each function. A typical layout of the RCC is shown in Fig. 5.3.1. The layout of the RCC is to be such that all the tools/ displays and indicators necessary for smooth control of the vessel from that position should be available to the operators.

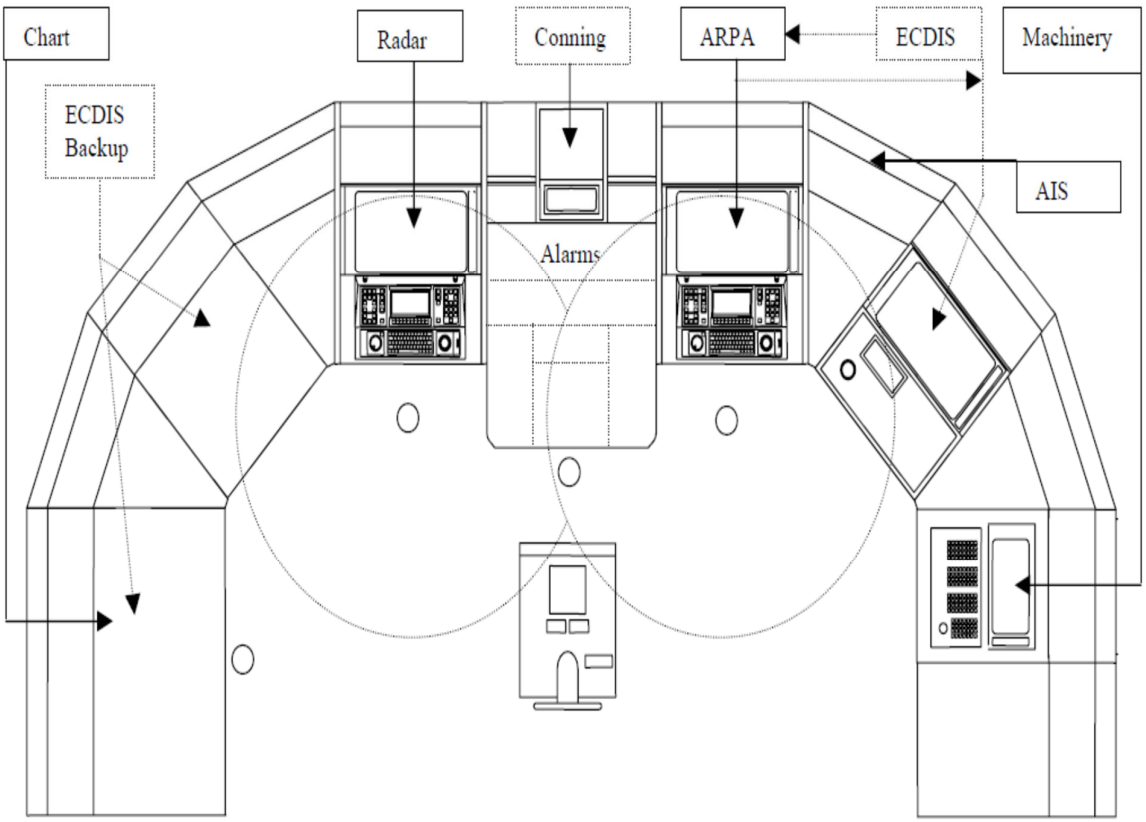


Fig. 5.3.1 : Typical Layout of RCC

5.3.2 Environmental Considerations for RCC

5.3.2 1 Internal environmental conditions in the RCC that may affect human performance are as follows:

a) - temperature
b) - humidity
c) - ventilation
d) - noise
e) - vibration
f) - illumination and type of lighting
g) - glare and reflection
h) - interior colours
i) - occupational safety

- The average noise level within the RCC is not to exceed 55 dB(A) during the length of the working day.
- The type of lighting is to be adequate for the tasks envisaged. Lux level between 500 to 800 is recommended. Lighting is not to create veiling reflections on displays or other reflective surfaces that require monitoring.
- Temperature and airflow is to be adjustable. As a guide, 'comfortable' temperature for office work is to be between 18.3°C and 20.0°C with airflow between 0.11 and 0.15 m/s.
- Sufficient cooling and ventilation is to be provided to protect electrical and electronics components of RCC from overheating.

5.4 Alarms and Monitoring

5.4.1 The RCC is to enable the operator to effectively monitor the behaviour of the ASV at all times, with a sufficient level of data to assess and actively respond to requests. Typical examples of the alarms and monitoring required (not limited to) are as follows:

5.4.2 Health status of ASV, including warnings and alerts:

- Built in Test Equipment (BITE) data presented to RCC;
- Battery status;
- Fuel level;
- Engine or equipment condition and performance warnings;
- Fire on-board.

5.4.3 Vessel operational status

- Navigational data:
- Machinery systems data
- Planned course
- Actual position, Heading, course over ground (CoG), speed over ground (SoG);
- Safety systems data

5.4.4 Situational Awareness data within vicinity of ASV; For example:

- Target/obstacle track data;
- Camera data;
- Radar data;
- In water sensor data (e.g. obstacle avoidance sonar);
- Sound data (e.g. warnings from other vessels).
- Collision avoidance:
- Warnings of potential obstacles.
- ASV intended action (autonomy level dependent)
- Attack or interference with the ASV or its subsystems.
- Chart overlays, including land ASV, shipping lanes, charted obstacles, seabed topography (if required).

5.4.5 The alarms are to provide enough information for the operator. Alarms are to be classified into different categories depending upon their priority levels.

5.4.6 Alarm messages are to be presented in a standard format, based upon existing Conventions. Alarm signals are to be at least 10 dB(A) over the background noise of the RCC.

5.4.7 Manning requirements of RCC are to be as per recommendations of the flag Administration when the vessel operations can be controlled from remote control centre.

5.5 Risk Assessment of RCC

5.5.1 The following possible risks are to be considered during RCC design, as a minimum. The list is only indicative and the risk assessment is to be specific to each project and location:

i. Situation awareness in the RCC: Errors due to not understanding the true situation of the vessel.
ii. Misunderstandings in interaction: latency in VHF communication, bad communication links, and language issues same as for manned systems, but worsened by lack of situation awareness.
iii. Delays in decision making due to lengthy time for operator to get into the loop (human-out-of the-loop syndrome).
iv. Location**:** Location of RCC is to be analysed in view of availability of network connectivity and communication links 24hrs in a day without disturbance
v. Corrupted backup data
vi. Human error in proper formatting of the backup medium or overwriting backup data
vii. Delayed recovery process due to backup tapes or disks being stored off site
viii. Accidental deletion of a file or software bug replicated to backup due to remote mirroring
ix. Cyber risks

5.6 Data Back Up and Recovery

5.6.1 Arrangements are to be provided at RCC to continuously record the changes in sensor data and the control commands together with the date and time stamps for each value. Data backup system at RCC is to be suitable for storing all collected data in a well defined format. Data is to be classified into engine data, bridge data, cargo data, video, images etc. and stored with time tag, function, data type for ease in recovery.

5.6.2 The centre should be designed for continuous data backup for minimum period of two weeks and facility should be provided for archiving and replay of backup data.

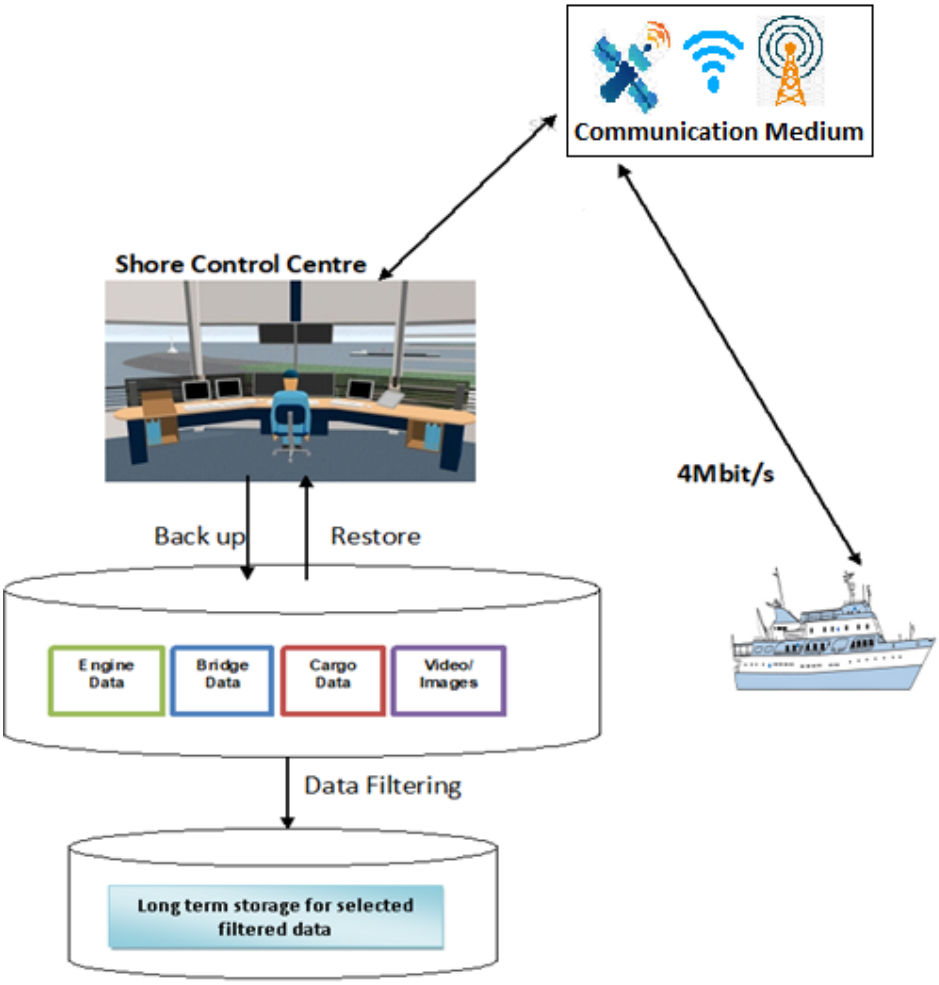


Fig 5.6 : Typical data storage and archival in RCC

Section 6

Tests and Trials

6.1 General

6.1.1 The verification and testing is to be carried out at different stages, such as

a) Design verification;
b) Testing on board following installation;
c) Harbour trials;
d) Sea acceptance trials;and
e) Subsequent testing during vessel's life.

6.1.2 Applicable requirements of the flag Administration/ statutory authorities are to be taken cognizance of whilst formulating the testing and trials plan.

6.2 Scope

6.2.1 The scope of verification and testing of the computer based systems is to include the following systems specific to autonomous notations and should be in addition to normal verification and testing as required by the relevant Rules:

i. All cabling and network devices
ii. All functionality relating to network communication by nodes connected to the network system
iii. All external and internal communications
iv. Monitoring and alarm systems
v. Backup procedures and results
vi. Verify effective response and recovery in the event of a failure of critical computer based system
vii. FMEA Proving trials
viii. Operations at remote control location including vessel control Centre communication
ix. Remote control
x. Autonomous controls
xi. Cyber security controls
xii. Contingency plans

6.2.2 The testing of major systems is to be carried out in following phases:

a) Simulation based testing for software
b) Hardware in loop testing
c) Integrated system testing on board at Harbour
d) Testing during sea trials from local and /or remote centre for all essential functions
e) FMEA trials

6.2.3 Test protocols for each phase are to be submitted for review prior to tests. Normal, abnormal and emergency conditions are to be simulated in each test phase and is to be in line with the operational concept document.

6.3 Network and Data Testing

6.3.1 The objective of the verification is to confirm through review of certificate and /or plans, the suitability of the network device for the intended operation in a marine environment. When requested, during onboard survey, the shipyard/system integrator is to submit relevant certificates to confirm that the equipment is designed, manufactured and tested as per the related standard.

6.3.2 The performance of the network is to be verified during on board survey as per reviewed test plan. Following tests to verify the network functionality and response are to be demonstrated onboard:

- Network loading
- Network storm test
- Redundancy tests where system is designed with redundant network and network devices
- Network monitoring
- Logical segregation of network. The testing is to include verification of security levels between zones.
- Where Demilitarized Zones (DMZ) are used, satisfactory functionality of DMZ to eliminate or reduces all direct communication between the control network zone and the other nonessential network zones is to be verified
- Testing of redundant networks.

6.3.3 Effective implementation of Network protection safeguards is to be demonstrated

6.3.4 Data storage, backup and recovery arrangement are to be tested for onboard and remote control centre as applicable.

6.3.5 Tests for communication systems used for data exchange are to be carried out to test the sufficiency of available bandwidth, latency, changeover to backup communication link in the event . Following tests would be required to be carried out

- Satisfactory communication between ship network and shore control centre
- Test and verify automatic transfer to backup link and data prioritization during loss of primary communication medium

6.4 Cyber Security

6.4.1 A test plan to verify the implemented controls is to be developed and tested. A copy of above documents is to be retained onboard and made available to IRS for subsequent verification during vessel life. After any cyber incident, changes in hardware and software, but not more than two year interval

6.4.2 Cyber Incident Response Measures

.1 The System Integrator and Supplier is to prepare a document to demonstrate satisfactory implementation of safeguards and instructions on how to verify their effective implementation, or a rationale for those not implemented.

6.4.3 A test plan to verify the implementation of controls is to be developed and tested during onboard survey.

6.4.4 A Vulnerability assessment and Penetration testing (VAPT) should be carried out for internal and external networks

6.4.5 Satisfactory operation of network devices to prevent unauthorized access from remote locations is to be verified during on board survey, as per approved test plan

6.4.6 Where systems are provided with remote maintenance arrangement and applicable security features are to be tested, for e.g.

- Session lock
- Auto log out function
- Blocking access during normal operation
- Monitoring remote maintenance activity

6.5 Software Maintenance

6.5.1 Subsequent to execution of software maintenance, following tests are to be carried out by the service provider for validation of new functionalities and/or improvements tests;

.

6.5.2 The tests are to ensure that the system under test:

- Performs intended functions
- Reacts safely in case of failures originated internally or by devices external to the system
- Interacts safely with other systems implemented on board vessel

6.5.3 The objective of software testing after maintenance is to verify that the equipment subject to software maintenance, integrated in the relevant system or sub-systems, behaves according to the specification and according to the applicable requirements.

6.5.4 During the software maintenance planning the producer of software or System Integrator and/or the Data Provider is to submit a Test Plan specifying the tests to be executed. Test cases covering both normal operation and failure conditions are to be specified in the Test Plan.

6.5.5 Test plans

6.5.5.1 The test plan is to identify the tests to be carried at developers' location and tests which can be demonstrated on board.

6.5.5.2 Where tests are carried out at developers place information/records of testing are required to be submitted. The tests which can be accepted based on records and which need to be witnessed are generally in accordance with Part 4, Chapter 7, Section 6 of IRS *Rules and Regulations for the Construction and Classification of Steel Ships*, however for autonomous controls IRS may require project specific approval.

6.5.5.3 The test plans should be developed considering following aspects as applicable

a. The Test Plan is to determine the scope and risks associated with the software maintenance and identify the objectives of testing, the method of testing, the expected time and resources required for the testing process.
b. It is to provide clear information on how the tests are carried out and how to verify the success or failure of each test.
c. Test cases are to be selected based on requirements, design specifications, risk analysis and interfaces of the equipment subject to software maintenance.
d. After the tests have been executed, the results of the executed tests are to be recorded, including the versions of the software under tests.
e. Test of procedures that can roll back to a previous software version and configuration during software maintenance, after a software update has been attempted to the shipboard equipment without success.
f. The results of the executed tests are to be discussed and analyzed in order to check which planned software updates can be delivered and to confirm that no failure has been detected during the test activities. In case of failure, corrective action is to be planned, and an updated Test Plan is to be submitted.
g. The process is to consider the implications and any risks associated that could result from

the rollback and identify appropriate testing performed post roll back in order to satisfy the administration and class of satisfactory working condition of the system. Rollback procedures are to be demonstrated to the satisfaction of IRS. Implementation of Roll back procedure for vessels above AUTN 1 level would require specific approval.

6.6 System Recovery

6.6.1Tests to demonstrate the necessary independence, functionality and operability of critical system are to be carried out during onboard survey

6.6.2 Verify that provision for a suitable Human Machine Interface (HMI) (communication means, controls, indications, alarms, etc as required) at each location where manual or local control is provided.

6.6.3 Review of each system to identify if safety functions are independent of control which could be affected in a Cyber Incident

6.6.4 Verify that Cyber Incident would not be destructive to equipment to the extent that it is unusable under manual backup.

References

- IMO MSC.1/ Circ. 1604: Interim Guidelines for MASS Trials
- IMO MSC.1/ Circ. 1638 : Outcome of the Regulatory Scoping Exercise for the Use of Maritime Autonomous Ships (MASS)
- ISO TR 11065
- Definitions of Autonomous ships Norwegian forum for Autonomous ships
- IMO MSC.1/Circ.1575 Guidelines for shipborne Position Navigation and Timing (PNT) data processing
- A pre analysis of autonomous ships by Danish Maritime Authority and Technical University of Denmark (DTU)
- UK code Maritime Autonomous surface ship
- IACS Recommendations 95 and 166
- IRS Classification Note: Type Approval of Electrical Equipment used for Control, Monitoring, Alarm and Protection Systems for use in Ships
- IRS Classification Note: Type Approval of Cyber Secured Control System Components
- IRS Guidelines on Certification of Software for Computer Based Control Systems
- IRS Guidelines on Maritime Cyber Safety
- IRS Guidelines on Cyber Safety for Land based Installations

End of Guidelines