DNV·GL

CLASS GUIDELINE

DNVGL-CG-0264 Edition September 2018

# Autonomous and remotely operated ships



DNV GL AS

# FOREWORD

DNV GL class guidelines contain methods, technical requirements, principles and acceptance criteria related to classed objects as referred to from the rules.



Any comments may be sent by e-mail to *rules@dnvgl.com*

# CHANGES – CURRENT

This is a new document.

# CONTENTS

# SECTION 1 GENERAL

## 1 Introduction

The area of autonomous and remotely controlled ship functions is developing fast. There are currently several industrial projects seeking to pilot the implementation of such technologies.

The societal expectations to the introduction of novel technologies are that these are implemented without adversely affecting the safety of people, properties and the environment, and that they do not negatively impact other aspects of society.

The instruments in use by the International Maritime Organization (IMO), governing the safety of commercial shipping do not provide any regulations for such novel technologies and operational concepts. A safety framework will have to be established by IMO before the benefits of the technologies with respect to reduced or no manning on board can be achieved for international shipping.

National or regional regulatory bodies are, however, free to support the introduction of novel technologies and operational concepts within their territorial waters. The same societal expectations for maintaining the safety will apply. This guideline has been developed to support the actors in the industry and the regulatory bodies in documenting and assuring a safe implementation.

The area of autonomy and remote operation of vessels is still an immature field where new ideas and technical solutions are being introduced. It is therefore currently not possible or desirable to provide detailed rules for all areas and combinations of concepts. Hence, the overall assurance process shall be risk based, but supported by functional and detailed technical guidance where possible. This guideline is planned to be further developed as more experience is gained from ongoing research-, newbuilding- and retrofitting projects.

In order to keep up with the latest developments, please contact DNV GL at *autoremoteships@dnvgl.com*.

## 2 Objective

The objective of this document is to provide guidance for:

1) safe implementation of novel technologies in the application of autonomous and/or remotely controlled vessel functions
2) recommended work process to obtain approval of novel concepts challenging existing statutory regulations and/or classification rules.

The overall intention is to provide a framework which ensures that application of such novel concepts and technologies result in a safety level equivalent to- or better than conventional vessel operations.

## 3 Scope

Sec.2 provides the main principles forming the foundation for DNV GL's approach for assessment of autonomous and remotely operated vessels.

Sec.3 describes processes to follow to obtain approval of designs applying novel technologies for autonomous and remote control of ship functions. The process described in Sec.3 [2] is intended for new operational concepts challenging statutory regulations with respect to minimum required manning. Sec.3 [4] describes a process for technology developers seeking verification of capabilities and performance of their technology.

The guideline also establishes a safety framework in form of technical guidance for such concepts and technologies. Sec.4 provides guidance to arrangements and technologies supporting remote control of navigation functions, while Sec.5 provides corresponding guidance for remote control of engineering functions. Sec.6 provides technical guidance to arrangements in the remote control centre. Technical guidance to the communication link connecting the remote control centre with the vessel, as well as technical guidance to other communication functions for the vessel and the remote control centre, is given in Sec.7.

Novel technology related to autonomous and remote control of vessel functions may enable a variety of new operational concepts. This edition of the guideline covers four types of concepts:

— *Decision supported navigational watch*

  This concept is based on enhanced decision support systems supporting an on-board officer in charge of the navigational watch in performing tasks for the navigation function. The incentive for such a concept may be to cover tasks conventionally done by the crew with advanced technology (e.g. look-out), or it may be for the purpose to enhance the safety and facilitate the officer in performing the navigation function.

— *Remote navigational watch*

  This concept is based on the tasks, duties and responsibilities of an officer in charge of the navigational watch being covered by personnel in an off-ship remote control centre. This concept assumes that no crew is available on board to support the remote personnel in performing the navigation function and the radio communication function as defined in the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW) code.

— *Remote engineering watch assisted by personnel on board*

  This concept is based on the tasks, duties and responsibilities of an officer in charge of the engineering watch being covered by personnel in an off-ship remote control centre. For this concept, it is assumed that crew is available on board to perform certain defined tasks and assist the remote personnel as needed.

— *Remote engineering watch*

  This concept is based on the tasks, duties and responsibilities of an officer in charge of the engineering watch being covered by personnel in an off-ship remote control centre. This concept assumes that no crew is available on board to support the remote personnel in performing the marine engineering function.

The above concepts may be linked to the degrees of autonomy used by IMO for their scoping exercise of maritime autonomous surface ships (MASS):

1) ships with automated processes and decision support
2) remotedly controlled ships with seafarers on board
3) remotely controlled ships without seafarers on board
4) fully autonomous ships.

# 4 Application

## 4.1 New operational concepts

This guideline may be applied by actors in the marine industry as the proposed process to follow and as safety framework to adhere to when seeking a flag administration's approval of operational concepts challenging statutory regulations. A flag administration may in the same way refer to this guideline for the process to follow and the safety framework to adhere to for approval of such concepts. The guideline may also be referred to by other organizations, such as coastal administrations, marine insurers, funding agencies, etc.

This guideline is based on the assumption that DNV GL has a role in supporting a project aiming at documenting equivalence between a new operational concept and a conventional concept, and at obtaining approval of the new operational concept. The guidance is founded on vessel designs complying with DNV GL main class rules and the verification processes leading to a class certificate for a vessel.

Class notations for the operational concepts described in [3] are under development. Until class notations have been established, a descriptive notation reflecting the operational concept, as provided for in DNVGL-RU-SHIP Pt.1 Ch.2 Sec.6, may be assigned to the vessel upon request.

## 4.2 Novel technology or novel application of technology

Developers of novel technology may apply this guideline with respect to the technology qualification process described in Sec.3 [4] and the technical guidance given in Sec.4 to Sec.7, in order to document and obtain verification of the capabilities and performance of the technology.

Also in the cases where conventional, known technologies are utilized in systems to enable novel operations, the technology qualification process described in Sec.3 [4] and the technical guidance given in Sec.4 to Sec.7, can be used to obtain verification of the capabilities and performance of the systems with regards to the novel application.

An approval in principle may be issued for technology subjected to the qualification process. The approval in principle will provide information on verified capabilities and performance of the technology, enabling the developer to offer the technology for new operational concepts intended enabled by such technology.

# 5 The roles of flag administrations and classification societies

## 5.1 General

Along with the novel technologies and the new operational concepts, new actors are emerging in the marine industry that may be unfamiliar with applicable safety regimes. There are also actors taking on new roles within the industry. The following is intended to provide an overview of applicable safety regimes in the context of autonomous and remotely operated ships.

## 5.2 Regulations

### 5.2.1 International maritime regulations

The International Maritime Organization (IMO) is an organization under the United Nations responsible for the regulatory framework for international shipping. The regulatory framework consists of legal instruments. The most well known instrument is the International Convention for the Safety of Life at Sea (SOLAS). The regulations apply to vessels engaged on international voyages.

### 5.2.2 National maritime regulations

Vessels engaged in domestic voyages within the jurisdiction of one coastal state only, are not subject to the international regulations set by IMO. The national regulations of the coastal state apply for such vessels. However, IMO Convention on the International Regulations for Preventing Collisions at Sea (COLREG) applies to all vessels.

## 5.3 Flag administrations

### 5.3.1 General

The flag state of a merchant vessel is the jurisdiction under whose laws the vessel is registered. The flag state has the authority and responsibility to enforce statutory regulations over vessels registered under its flag, and has the authority and responsibility to issue the statutory certificates for the vessel. The statutory certificates may either be international voyage certificates based on compliance with IMO regulations, or domestic voyage certificates based on compliance with national maritime regulations.

### 5.3.2 Exemptions and approval of equivalence from IMO regulations

For vessels engaged on international voyages subject to IMO regulations, the authority of the flag administration to give exemptions from requirements or approve equivalence with requirements, is described in the IMO instruments. The three instruments of particular interest for this guideline are described below:

— International Convention for the Safety of Life at Sea (SOLAS)

The administrations may give exemptions from provisions given in Ch.II-1, Ch.II-2, Ch-III and Ch-IV for ships embodying features of novel kind, see SOLAS Ch-I / Reg.4. The ship shall comply with safety requirements adequate for the intended service. This is subject to consideration by both flag administration and government of the states intended visited by the ship.

The flag administration has the authority to approve equivalent fittings, materials, appliances and apparatus being at least as effective as those required by the regulations, see SOLAS Ch-I / Reg.5.

— International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW)

The STCW convention provides regulations for crew competencies and requires that an officer in charge of the navigational watch shall be physically present on the navigating bridge:

*2. Administrations shall require the master of every ship to ensure that watchkeeping arrangements are adequate for maintaining a safe watch or watches, taking into account the prevailing circumstances and conditions and that, under the master's general direction:*

*.1 officers in charge of the navigational watch are responsible for navigating the ship safely during their periods of duty, when they shall be physically present on the navigating bridge or in a directly associated location such as the chartroom or bridge control room at all times;*

*(STCW Reg. VIII/2)*

Reg. I/13 of the convention opens for flag administrations to give exemptions from the regulations for ships engaged in particular trials. Details of the trials shall be reported to IMO at least 6 months before the trials commences. Any IMO member state may object to the trials, which means that the trials can not be conducted within the waters of an objecting coastal state. The flag administration may upon successful trials authorize the ship to continue the operations permanently.

A condition for conducting the trials and for continued permanent operations is that the trials and operations are conducted in accordance with guidelines adopted by IMO. Accordingly, flag administrations do not have authority to authorize such trials and permanent operations for a ship until IMO has adopted related guidelines.

— Resolution A.1047(27) - Principles of minimum safe manning

Manning is regulated by SOLAS Ch.V, Reg.14, and the ISM Code, Part A, 6.2.2, which both refer to Assembly Resolution A.1047(27) *Principles of Minimum Safe Manning*. These guidelines take into consideration levels of automation and support from on-shore in deciding safe manning:

- *1.1 The minimum safe manning of a ship should be established taking into account all relevant factors, including the following:* [...]
- *.3 level of ship automation;* [...]
- *.10 degree of shoreside support provided to the ship by the company;* [...]

*(IMO Res. A.1047(27) Annex 2)*

- *1.1 The administration may require the company responsible for the operation of the ship to prepare and submit its proposal for the minimum safe manning of a ship in accordance with a form specified by the administration.*

*(IMO Res. A.1047(27) Annex 3)*

In submitting the proposal for the minimum safe manning to the flag administration, the owner may refer to this guideline for the process that shall be followed and the safety framework that shall be adhered to.

### 5.3.3 Exemptions and approval of equivalence with national maritime regulations

Vessels engaged in domestic voyages within national waters of a coastal state are subject to the national regulations/laws of the coastal state. The national maritime administration / national coastal administration may have been granted permission to exempt ships in domestic voyages from the national regulations/laws. Such delegation of authority will vary between states.

## 5.4 Classification societies

### 5.4.1 The role of class

#### 5.4.1.1 General

Classification societies develop and maintain technical standards (rules) for the design, construction and maintenance of ships. The main class rules cover technical requirements to structure, watertight integrity, machinery, auxiliary systems, pressure equipment, electrical systems and control systems. The classification society carries out verifications in form of design approval and surveys to establish reasonable assurance that a vessel, with its systems and components, is constructed in accordance with the rules. Upon entry into operation, the vessel is assigned class and a classification certificate is issued for the vessel. The vessel is further surveyed by the classification society in order to establish reasonable assurance that the applicable requirements are met and class can be maintained.

SOLAS Ch.II-1 requires that vessels are designed, constructed and maintained in compliance with the structural, mechanical and electrical requirements of a classification society which is recognized by the administration, i.e. a classification society certificate is required for vessels engaged in international voyages.

The main class rules cover in general the scope of SOLAS Ch.II-1. The remaining parts of SOLAS (e.g. fire protection, life-saving appliances, safety of navigation etc.) are in general not covered by the main class rules.

#### 5.4.1.2 Exemptions and approval of equivalence

DNV GL reserves the right to interpret, decide equivalence or make exemptions from own rules.

### 5.4.2 The role of recognized organizations

#### 5.4.2.1 General

Flag administrations may recognise organisations to carry out inspections and surveys of vessels on their behalf for compliance with statutory regulations. The recognised organisation will then issue statutory certificates confirming compliance with the statutory regulations in the role as recognised organisation (RO) on behalf of the flag state.

Certain statutory certificates may not be part of the delegation as RO. The scope of delegation is specified in agreements between each flag state and their ROs. Minimum safe manning on board ships is regulated by IMO / national regulations. Manning is not within the scope of a class society, and is not delegated to class societies acting as RO on behalf of an administration. Safe manning certificates are issued by flag states.

#### 5.4.2.2 Exemptions and approval of equivalence

The RO does not have authority to give exemptions from statutory regulations. Exemptions from statutory requirements are given by the flag administration in accordance with [5.3].

ROs may be delegated authority to approve equivalencies. This depends on the scope of delegation in the agreement between the flag administration and the RO. When this authority is not delegated, the RO will normally receive the equivalence request from the builder and forward the request to the administration together with RO's own evaluation and recommendations.

# 6 References

**Table 1 External references**

| *Document code/URL* | *Title* |
|---|---|
| https://www.sintef.no/projectweb/criop/the-criop-methodology/ | *CRIOP method description* |

| Document code/URL | Title |
|---|---|
| https://www.faa.gov/regulations_policies/handbooks_manuals/aviation/risk_management/ss_handbook/media/Chap8_1200.pdf | *Operating and support hazard analysis (O&SHA) method description* |

**Table 2 DNV GL references**

| Document code/URL | Title |
|---|---|
| DNVGL-RP-A203 | *Technology qualification* |
| DNVGL-CP-0507 | *System and software engineering* |
| DNVGL-RU-SHIP | DNV GL rules for classification of ships |

# 7 Definitions

## 7.1 Definition of verbal forms

**Table 3 Definitions of verbal forms**

| Verbal foms | Definition |
|---|---|
| shall | verbal form used to indicate requirements strictly to be followed in order to conform to the document |
| should | verbal form used to indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required |
| may | verbal form used to indicate a course of action permissable within limits of the document |

The verbal form *should* is used in general in this document, as this is a guideline describing recommended processes to follow in order to document equivalence with conventional designs.

The verbal form *shall* is used in this document when referring to statutory or class requirements that are applicable. This is typically used in Sec.2 [2] describing requirements for equivalent level of safety that shall be achieved for alternative designs, and in the baseline requirements in Sec.4 to Sec.7 where statutory and main class requirements forming the basis for the equivalence that shall be achieved, are described.

## 7.2 Definition of terms

**Table 4 Definition of terms**

| Terms | Definition |
|---|---|
| anticipated failure | failure expected to occur that should not prevent normal operation of the vessel |
| approval in principle (AiP) | statement of verification normally issued after a technology qualification process |
| approval of manufacturer | certification scheme to verify a manufacturer's ability to deliver products according to specific standards and rules |

| *Terms* | *Definition* |
|---|---|
| autoremote | umbrella adjective to denote any operation, task, function or system where the intention is to create additional decision support, remote-control, or autonomous functionality compared to a conventional, crewed ship |
| autoremote function | vessel function that is under remote operation from an off-ship remote control centre<br>The function may be autonomously controlled by a system or manually controlled by the remote operator, or a combination of the two. |
| autoremote infrastructure | whole set of vessel(s), systems, communication-link(s), remote control centre and all other systems that together fulfils all the requirements and intentions of a safe operation of an autonomous or remotely operated vessel |
| autoremote system | any system, on or off a ship which implements one or more autoremote function |
| autoremote vessel | vessel for which one or more key functions are remotely controlled from a remote control centre, possibly by assistance from personnel on board<br>To support safe and efficient operation of the vessel, the remotely controlled key function(s) is arranged with a defined level of automation ranging from simple decision support to complete automatic control. The extent of support from on-board personnel and the level of automation should be detailed in document *Concept of Operation* (CONOPS)". |
| bow-tie analysis | risk evaluation method, visualizing threats, barriers and consequences related to an unwanted event caused by a hazard |
| crisis intervention and operability analysis | methodology used to verify and validate the ability of a control centre to safely and efficiently handle all modes of operations including start up, normal operations, maintenance and revision maintenance, process disturbances, safety critical situations and shut down |
| event tree analysis | risk analysis method described in standard textbooks and e.g. in IEC 62502:2010 |
| fault tree analysis | hazard identification and analysis technique described in standard text books and e.g. in IEC 61025:2006 |
| hazard and operability study | hazard identification technique described in standard text books and e.g. in IEC 61882:2016 |
| hazard identification | common term used for FMEA, FMECA, SWIFT, What If + Checklist, HAZOP and several other methods described in various textbooks and industry standards |
| hidden failure | failure that is not immediately evident to responsible personnel and has the potential for failure of equipment to perform an on-demand function, such as protective functions in power plants and switchboards, standby equipment, backup power supplies or lack of capacity or performance |
| key functions | see Sec.2 [6] |
| minimum risk condition (MRC) | see Sec.2 [5] |
| novel technology | technology, products or systems for which complete performance or approval criteria does not exist |
| Operating and maintenance hazard analysis | same definition as for operating and support hazard analysis |
| operating and support hazard analysis | analysis used to identify and evaluate the hazards associated with the environment, personnel, procedures, operation, support, and equipment involved throughout the total life cycle of a system/element |

| Terms | Definition |
|---|---|
| operational design domain | The different conditions and scenarios that the vessel or a function is designed to manage |
| operational status | indication of an autoremote function or system's status with regards to its ability to perform at normal capacity |
| potential failure | failures that are less probable than anticipated failures, but may still occur sometime during the vessel's operational life |
| responsibility mode | set of pre-defined modes that indicates to what degree a remote operator is expected to manage a specific autoremote function or system<br>Typical responsibility modes are: remote control, supervision, monitoring, decision support. |
| use-case | list of actions or steps typically defining the interactions between a role and a system to achieve a goal.<br>Use-cases may be used as a part of the requirements specification for a system. |

## 7.3 Definition of symbols

## 7.4 Abbreviations

**Table 5 Abbreviations**

| Abbreviation | Description |
|---|---|
| A | autonomous, see Sec.4 Table 1 |
| AiP | approval in principle, see definition of terms in Table 4 |
| AIS | automatic identification system |
| AoM | approval of manufacturer, see definition of terms in Table 4 |
| AO | automatic operation, see Sec.5 [1.2] |
| AS | automatic support, see Sec.5 [1.2] |
| AVA | algorithm-based verification agent |
| AVR | automatic voltage regulator |
| BAM | bridge alert management |
| BITE | built-in test equipment |
| BNWAS | bridge navigational watch alarm system |
| CAM | central alert management |
| CCTV | closed-circuit television |
| CMC | certification of materials and components |
| CONOPS | concept of operations |
| CPA | closest point of approach |
| CQ | concept qualification |

| *Abbreviation* | *Description* |
|---|---|
| COTS | commercial off-the-shelf |
| CRIOP | crisis intervention and operability analysis, see definition of terms in Table 4 |
| DMZ | demilitarized zone |
| DP | dynamic positioning |
| DS | decision support, see Sec.4 Table 1 |
| DSE | decision support with conditional execution capabilities, see Sec.4 Table 1 |
| ECDIS | electronic chart display and information system |
| ENC | electronic navigational chart |
| EPFS | electronic position fixing system |
| ETA | event tree analysis, see definition of terms in Table 4 |
| FAT | factory acceptance test |
| FiS | fleet in service |
| FMEA | failure mode and effect analysis, see Sec.3 [4.3.3.3] |
| FOV | field of vision |
| FTA | fault tree analysis, see definition of terms in Table 4 |
| GMDSS | global maritime distress and safety systemarbour acceptance test |
| GNSS | global navigation satellite system |
| HAZOP | hazard and operability study, see definition of terms in Table 4 |
| HAZID | hazard identification, see definition of terms in Table 4 |
| HCS | heading control system |
| HIL | hardware-in-the-loop |
| HMI | human-machine interface |
| HSC | high-speed craft |
| HVAC | heating, ventilation, and air conditioning |
| HW | hardware (computer hardware) |
| IMO | International Maritime Organization |
| INS | integrated navigation system |
| IT | information technology |
| LRIT | long-range identification and tracking |
| M | manual, seeSec.4 Table 1 |
| ML | machine learning |
| MRC | minimum risk condition (vessel safe state), see Sec.2 [5] |
| NB | a vessel newbuilding |

| *Abbreviation* | *Description* |
|---|---|
| NDSS CA-GA | navigation decision support system for collision- and grounding avoidance |
| O&SHA | operating and support hazard analysis |
| OOW | officer of the watch |
| OT | operation technology |
| PLC | programmable logic controller |
| RCC | remote control centre |
| RO | recognized organization |
| ROTI | rate-of-turn indicator |
| SAT | seatrial acceptance test |
| SC | self-controlled, see Sec.4 Table 1 |
| SDLC | software development life cycle |
| SIL | software-in-the-loop |
| SOG | speed over ground |
| SQuaRE | systems and software quality requirements and evaluation, ref. ISO/IEC 25000 |
| SRS | sound reception system |
| STW | speed through water |
| SW | software |
| TA | type approval |
| TCPA | time to closest point of approach |
| THD | transmitting heading device |
| TQ | technology qualification |
| UPS | uninterrupted power supply |
| VDR | voyage data recorder |
| VHF | verification and validation |
| VLAN | virtual local area network |
| VTS | vessel traffic service |

# SECTION 2 MAIN PRINCIPLES

## 1 General

The following main principles form the foundation for DNV GL's approach for assessment of autonomous and remotely operated vessels (autoremote vessels):

— equivalent safety
— risk-based approach
— operational focus
— minimum risk conditions
— functional focus
— degrees of automation and human involvement per function
— system engineering and integration
— design principles
— software engineering and testing
— cyber security.

The above listed principles are explained in following subsections and linked to both the process guidance and technical guidance given in the rest of the document.

## 2 Equivalent safety

New vessel operational concepts based on autonomous and remote control of vessel functions shall have a level of safety equivalent or better, compared to conventional operations of vessels with respect to safeguarding life, property and the environment.

When considering safety measures for a vessel, the risks associated with the new operational concepts shall not focus only on consequences for the on-board crew, but also take into consideration consequences for the public, the assets and the environment. An equivalent or better level of safety shall be obtained in all these respects.

For unmanned vessels, it has in some cases been argued for reduced safety measures in view of the absence of humans on-board. Some conventional safety measures are intended solely to safeguard the crew (e.g. lifeboats and lifejackets), and may be omitted for unmanned vessels without affecting safety in any respect. Other conventional safety measures may however contribute to safety for the public, the assets or the environment. As an example, safety measures such as fire extinguishing capabilities have been proposed reduced considering the absense of humans on board. Reduced fire extinguishing capabilities will however have impact on the risks for the assets and possibly for public and environment. This is not in line with DNV GL's general approach aiming at ensuring an equivalent or better safety level. If, however a more lenient approach is proposed for a specific vessel or operation, the increased risks and their consequences will be subject to acceptance by relevant stakeholders, e.g. vessel insurance and coastal administration.

Sec.4 through Sec.7 provides guidance for technical design and construction of systems and components supporting autonomous and remote control of vessel functions, with the objective to obtain a safety level for the vessel equal to or better than that of a conventional vessel.

## 3 Risk-based approach

Considering that new vessel operational concepts based on autonomous and remote control of vessel functions are associated with novelty, immaturity and complexity, it is necessary to focus on identifying and mitigating the risks associated with the new introduced operations, functionality and systems.

Structured risk-analyses should be performed on several abstraction-levels, typically utilizing several different risk-analysing methodologies:

- Risk analysis covering the operational concept of the vessel, identifying risks and mitigation associated with the proposed division of responsibility between the automatic systems and personnel in different locations. Here also the proposed minimum risk conditions (MRCs) are examined in detail.
- Risk analysis associated with design and implementation of novel technology controlling vessel functions. The focus is on the safe-state, failure modes and fault robustness of the functions and systems.
- Risk analysis associated with the remote supervision and control of a vessel or system from a remote control centre. The risk analysis should specifically focus on the RCC and its supporting systems and demonstrate that any failures thereof will be managed safely by automation systems or personnel on board.

The deliverables of these risk analysis activities are outlined in Sec.3 [2] and Sec.3 [4] respectively.

All identified risk-mitigation activities must be systematically followed-up and tracked to conclusion, normally with a verification activity which proves that the actions in question will mitigate the risks as intended.

## 4 Operational focus

As automatic control of functions replaces operations traditionally performed by humans, operational modes and scenarios in question should be thoroughly analysed to identify all relevant variations and potential hazards.

Traditionally, an automated function generates an alarm when something is wrong or goes out of bounds, and it is responsibility of the human operator to take appropriate actions to manage and rectify the situation. As the human operator is partly or wholly replaced by technical arrangements, remote- and autonomous operations are expected to manage a greater variety in the operations. The ship systems should be designed so that the extent and need for alarm- and monitoring functions correspond to the actual (often limited) possibilities for manual intervention.

It becomes essential to analyse the operational aspects up-front to ensure that the applied technology will be able to deal with all reasonably foreseeable events.

The process outlined in Sec.3 [2] requires start of such analysis at early stages and that it is documented in the concept of operation (CONOPS), with the safety related aspects further detailed in the safety philosophy document.

## 5 Minimum risk conditions

When establishing autoremote functionality it is important to determine how the ship and its functions should react in all relevant situations (as described in [4] above).

In some cases, events may force the ship or other parts of the autoremote infrastructure out of its normal operation. In such an event, it is essential that the relevant response is defined, and that the ship is put in a state that poses the least risk to life, environment and property. These states are called minimum risk conditions (MRCs).

A minimum risk condition (MRC) is a state that the ship should enter when the autoremote infrastructure experiences situations that are outside those in which it can operate normally, but is still expected to deal with in one way or another.

An MRC can be looked upon as a safe state for the vessel and is a part of a contingency plan (see Sec.4 [6]).

Most MRCs are expected being active, where the vessel and its important systems remain active, albeit with (some) reduced capabilities.

The vessel is typically pushed from a normal operational state through an abnormal situation and further to MRC-states by events, either caused by changes in the environment (e.g. deteriorating weather) or by failures / incidents (e.g. loss of a propulsion system). It is also possible that an event puts the ship back in normal operation after it has been in an MRC state (e.g. improving weather or restoration of propulsion).

There may be several viable MRCs for a specific event depending on e.g. the vessel's operational status, location, and external conditions. These MRCs should be organised in a hierarchy with clear decision paths between them. The most relevant (hierarcy of) MRC(s) may be decided in real-time during the operation/ voyage. The MRC which makes up a leaf of the hierarchy (where no further change in state is possible or desired) is referred to as last resort MRC.

If a specific MRC cannot be sustained for an indefinite period of time, it is normally not accepted as a last resort MRC.

When navigating waters that are congested or have high traffic, it is expected that the vessel has at least two MRCs available at any time during normal operations.

External events, failures or incidents considered potential (see Sec.3 [2.4]) should not force the vessel outside of last resort MRC.

Anticipated events should not force the vessel to an MRC, but allow the vessel to maintain normal operation or to handle abnormal situations. See also design principles in Sec.3 [2.4].

The definition and analysis of relevant MRCs is done in each concept qualification project during the first phases (see Sec.3 [2.3] and Sec.3 [2.4]).

Design of system redundancy and fault tolerance should be decided based on the defined MRCs. See also guidance for risk assessment in Sec.3 [2.4].

To illustrate the concept, a list of some possible MRCs is provided in App.A.

Figure 1 illustrates the concept of normal operation, abnormal situations and MRCs.

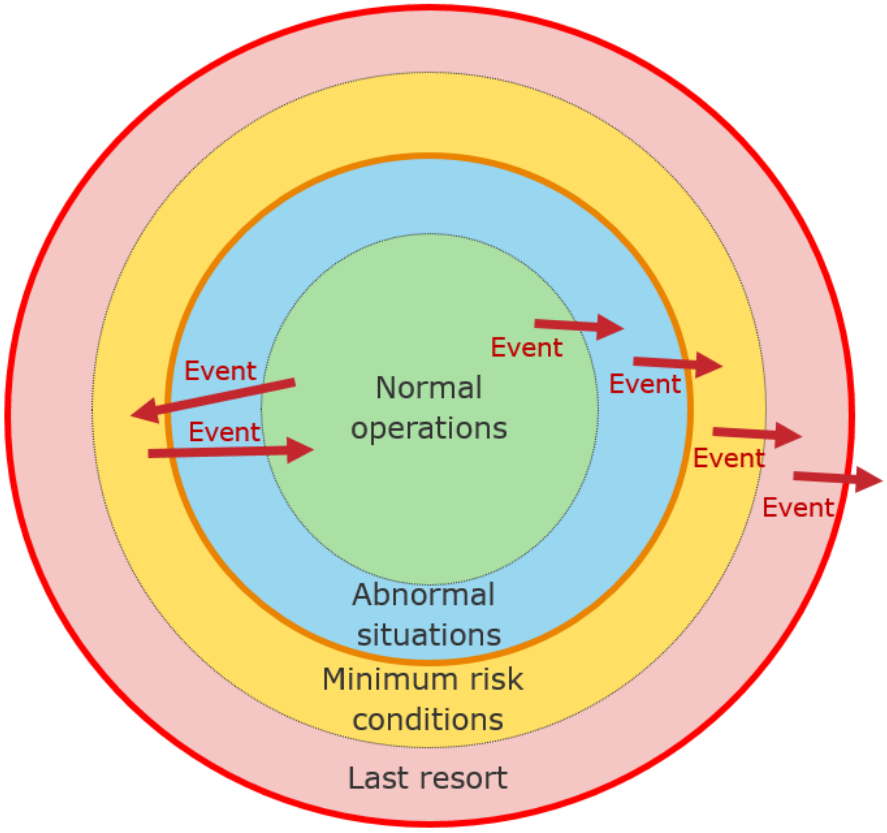


**Figure 1 Concept of normal operation, abnormal situations and MRCs**

## 6 Functional focus

Given that a risk-based approach should be applied with an operational focus to achieve an equivalent level of safety, the design methodology should specifically address all functions of the autoremote infrastructure needed to achieve this objective. Some of these functions are traditional ship-functions, others are related to the automatic and remote operation.

The below list intends to identify such key functions. The list is not exhaustive and may be extended, depending on e.g. vessel type and the intended level of autonomy and remote operation.

Key functions of the autoremote infrastructure:

— remote control and supervision
— communication
— navigation and maneuvering
— propulsion
— steering
— electrical power supply
— control and monitoring
— watertight integrity
— fire safety
— ballasting
— drainage and bilge pumping
— anchoring
— cargo handling
— maintenance.

The functions listed above are on a high abstraction level, and it is often desirable to make only parts of these functions remote-controlled or autonomous. A further analysis of the function is then needed to identify the different parts that should be automatic, autonomous, remote-controlled or manual.

This detailing of the functions starts already during the analysis of the operational aspects, where individual tasks and sub-functions are identified to be performed automatically or remotely. The document concept of operation (CONOPS) is used for this purpose, see Sec.3 [2.3.1].

Later, a further detailed decomposition is performed, this is outlined in App.B and further detailed in Sec.4 [1.3] and Sec.5 [1.2].

## 7 Degrees of automation and human involvement per function

Several scales have been developed to describe the level of autonomy for ships. Most scales assume the vessel to adhere to a specific level or autonomy and do not consider differences between vessel functions.

A suitable categorization of self-controlling capabilities will depend on the context it is used in, and may be different for e.g. navigation and machinery functions. Navigation is conventionally based on a high degree of human observations, analysis and decisions, while the machinery functions are to a high degree fully self-controlled and operating under supervision by the crew.

This guideline is using different categorizations for the degrees of automation for respectively the navigation functions and the engineering functions. The technical guidance for the navigation functions in Sec.4 is based on a categorization in line with what is established in the vehicle automation industry (see Sec.4 [3]). A simpler categorization is used for the engineering functions in Sec.5, distinguishing between systems providing automatic support and systems performing automatic operation.

To facilitate a stepwise introduction of autonomous and remote-controlled functionality not only for newbuildings, but also for retrofitting of existing vessels, in this guideline technical guidance for navigation functions in Sec.4 and for engineering functions in Sec.5 is structured based on a systematic decomposition of the key functions listed in [6].

## 8 System engineering and integration

The anticipated complexity of applying new technology for new operational concepts warrants a high focus on system engineering and integration activities. The organization taking on the role as system integrator should be clearly identified in each concept qualification project. The system integrator should be responsible for the overall functional design and for verifying and validating the autoremote functionality with focus on the operation and safety of the vessel.

Details about the system integrator's responsibilities are found in Sec.3 [2].

## 9 Design principles

The following principles should govern the design of autonomous or remotely operated vessels.

1) Maintain a safe state.

   No incidents, including fire and flooding on board or in the remote control centre, or single failure in systems on board or systems interfacing the vessel, should cause an unsafe mode for the vessel or its surrounding environment. It should be possible to enter and maintain a minimum risk condition (MRC) in all operations and scenarios defined in the document concept of operation. Considering that different minimum risk conditions may apply in the various operational phases/modes, the design should be based on all defined MRCs. See Sec.5 [3].

2) Maintain normal operation.

   Anticipated failures should not prevent normal operation of the vessel. Normal operation should be defined in the document concept of operations (CONOPS) and may imply reduced capacity.

3) Redundancy and alternative control.

   The capability to maintain safe state (within MRC) should not be based only on fail-to-safe properties of a single system or component. Any single failure or incident should be mitigated by applying redundancy principles (e.g. two steering systems) or alternative control capabilities (e.g. loss of collision avoidance is mitigated by position keeping).

4) Independent barriers.

   Systems or components which are designed with redundancy to comply with the above principles should be mutually independent. This includes segregation in accordance with fire/flooding scenarios in Sec.5 [3].

   If failure of a function is mitigated by alternative control capabilities, there should not be any common mode failures or incidents affecting both functions simultaneously.

5) Self-contained capabilities on board.

   Failure of remote systems should be mitigated by systems or personnel on board. Normal operation or safe state should be maintained by use of automation systems and/or personnel on board.

6) Self-diagnostics and supervision.

   Enhanced diagnostic functions and advanced alert management functions should be implemented to prevent undetected failures and ensure sufficient supervision.

The above principles should be addressed in relevant documents such as safety philosophy/related risk assessment and give rise to e.g. fault tolerant design where applicable. See Sec.3 [2].

Specific guidance related to failure modes, redundancy, independence and safe states is given in the technical guidance sections (see Sec.4 to Sec.7).

## 10 Software engineering and testing

Even for conventional vessels there has been an increasing trend for several years to rely on software and communication networks in control, monitoring and safety functions on board. It is evident that autoremote vessels will be completely dependent on such technology.

The trend has also shifted from use of dedicated programmable logic devices with proprietary programming languages to more common use of general purpose computers and programming languages.

Due to such increasing integration and use of complex, software-based systems it is widely recognized that quality assurance of the development, delivery and modification of software-based systems is important to ensure safe and reliable vessel operation.

There are basically two supplementary ways of managing the quality of software. One is to inspect and test the end-product for defects, the other is to control the software development and configuration process to prevent the mistakes from being made in the first place.

For functionality related to autonomous and remotely operated ships, DNV GL recommend that both methods are utilized extensively. It is required that the software is being developed and configured according to established processes, and that a verification and validation strategy which puts emphasis on elaborate, multi-faceted testing of the software is established. These items are reflected in the processes for concept qualification and technology qualification described in Sec.3 [2] and Sec.3 [4].

## 11 Cyber security

The increased communication between the vessel and remote systems is bringing with it a concern about the cyber security for the related systems. In order to address this concern, the guideline puts emphasis on securing the systems when it comes to cyber security. Both the concept qualification process (Sec.3 [2]) and the technology qualification process (Sec.3 [4]) includes cyber security aspects in the risk analysis, and the technical guidance for the communication link (Sec.7) references both the type approval programme for cyber security and the cyber security class notation.

The design of both the overall autoremote infrastructure and the individual systems should explicitly take cyber security aspects into account. The general rule is that a defence in depth concept should be applied, where multiple layers of mechanisms, functions and barriers together aim at hindering, detecting and limiting the damage of cyber security breaches.

The infrastructure of network components, servers, operator stations and other endpoints should be explicitly configured and hardened to reduce the likelihood and consequences of cyber security breaches. This applies both on board and in any remote control centre.

It may also be relevant to assess the cyber security of IT service providers, telecom providers, hosting services, external servers, relay stations, satellites, etc , depending on scope of the project.

# SECTION 3 QUALIFICATION AND APPROVAL PROCESS

## 1 Introduction

When new operational concepts enabled by novel technology are introduced, the solutions may not meet existing regulations and technical requirements. The technology may also be intended to perform a function that is traditionally performed by humans, and for which no performance requirements to the technology have been developed.

To support development and introduction of such new operational concepts and novel technology in ship designs, both class rules and statutory regulations provide guidance on processes to follow for obtaining approval of alternative designs in general. The objective of these processes is to document that a new concept with its enabling technology will provide a level of safety equivalent or better compared to a conventional vessel designed and operated in accordance with existing rules and regulations, see Figure 1.

This section provides further descriptions of processes that may be followed to obtain the approvals. Three processes are described:

— Concept qualification.

  Applicable to new operational concepts as proposed by a concept submitter, where the new proposed operations challenge statutory regulations, typically with respect to required crew on-board ships. The flag administration is part of this process, as exemptions from statutory regulations and final approval of the new operational concept lays with the flag administration. The concept qualification process is described in [2].

— Approval of conventional technology.

  Applicable to conventional technology used in conventional ways. Covered by other class processes and only included and briefly described in this guideline for the sake of completeness. See [3].

— Technology qualification.

  Applicable to novel technology related to autonomous and remote control of ship functions. The technology qualification process has the objective to document properties of a system and to ensure safe implementation of the technology with respect to any negative effects on the respective vessel functions. The technology qualification process is a process between the developer of the technology and DNV GL. Use of the technology to enable a new operational concept for a ship is not part of this process, but belongs to the concept qualification process subject to approval by the flag administration. The technology qualification process is described in [4].

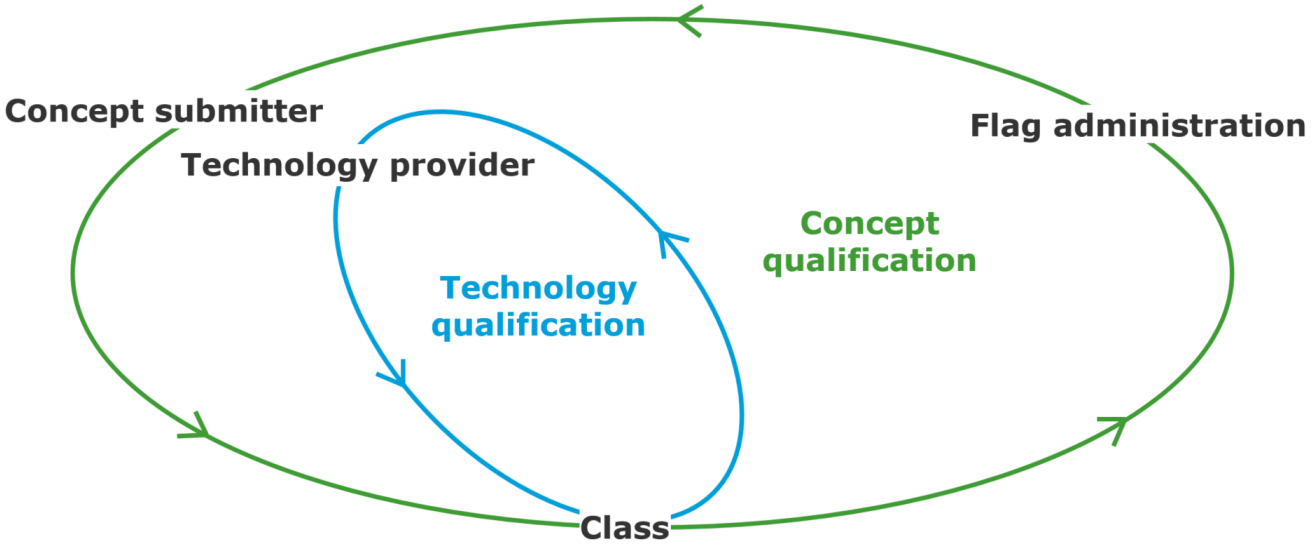


**Figure 1 Interactions of processes and actors for concept and technology qualifications**

New operational concepts are today introduced based on technologies that are still under development. It is foreseen that the technology and concept developments will go hand-in-hand for the first pilot projects, where the properties of the technologies will be scrutinized on pilot vessels, and operational concepts for the pilot vessels adjusted accordingly. This may result in a more integrated qualification process for the technologies and the concept for the first pilot projects.

The purpose of dividing the technology and concept qualifications into two processes is to provide for a modular approach. In this way technology developers may obtain approval of their technology with defined properties that may be applied in different types of operational concepts, and new operational concepts may be developed based on the properties of available approved technologies.

Figure 2 provides examples on how technology modules may be combined to support new operational concepts.

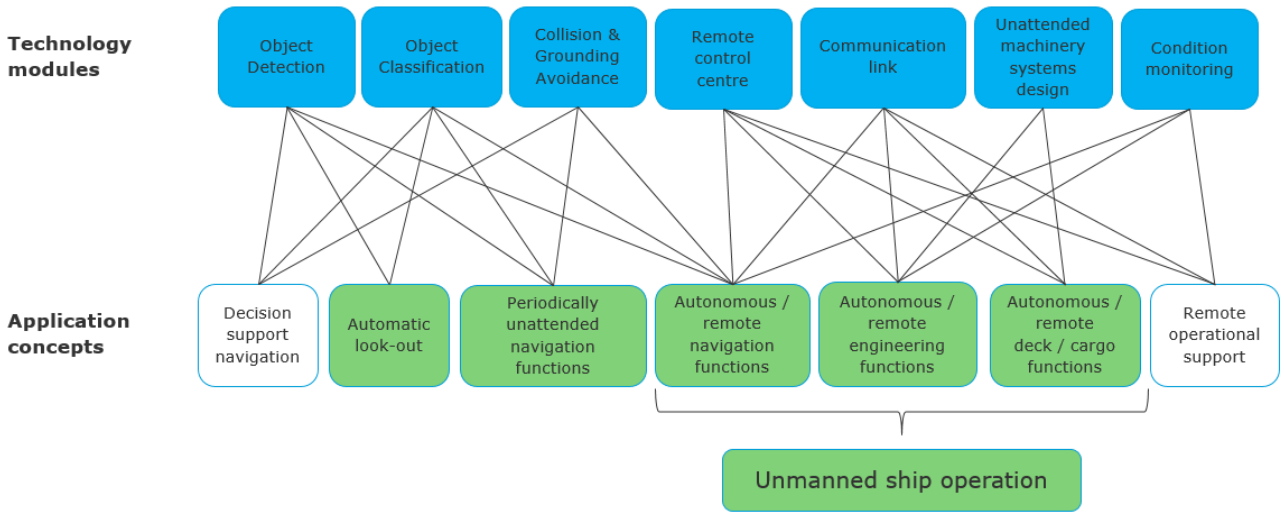


**Figure 2 Combinations of technology modules into new operational concepts**

# 2 Concept qualification process

## 2.1 General

This section describes a process where DNV GL takes on a 3rd party role between the concept submitter and the flag administration, with the purpose to aid the project in documenting and verifying that the proposed concept achieves an equivalent or better safety level compared with conventional operation of a vessel.

This part of the guideline is applicable for concepts where tasks normally performed by on-board crew are intended to be replaced by autonomous or remote control of vessel functions, with or without assistance from personnel on-board.

New operational concepts where qualified crew is intended removed from the ship will challenge statutory regulations. Manning is regulated by IMO Assembly Resolution A.1047(27) *Principles of Minimum Safe Manning*. As described in Sec.1 [5], manning is not in the scope of class. The safe manning certificate is issued by the flag state, and related exemptions / approval of equivalents are accordingly in the responsibility of the flag administration to grant.

In submitting the proposal for the minimum safe manning to the flag administration, the concept submitter may refer to this guideline for the proposed process to follow and the safety framework to be adhered to. It will then be up to the relevant flag administration for the specific project whether to accept to follow the process described in this guideline, to specify additional control measures, or to provide its own specification of the process that shall be followed.

An illustration of the relationship between the concept submitter, DNV GL and flag administration is shown in Figure 3. The overall process is following the principles in IMO MSC.1/Circ.1455 *Guidelines for the approval of alternatives and equivalents as provided for in various IMO instruments*.

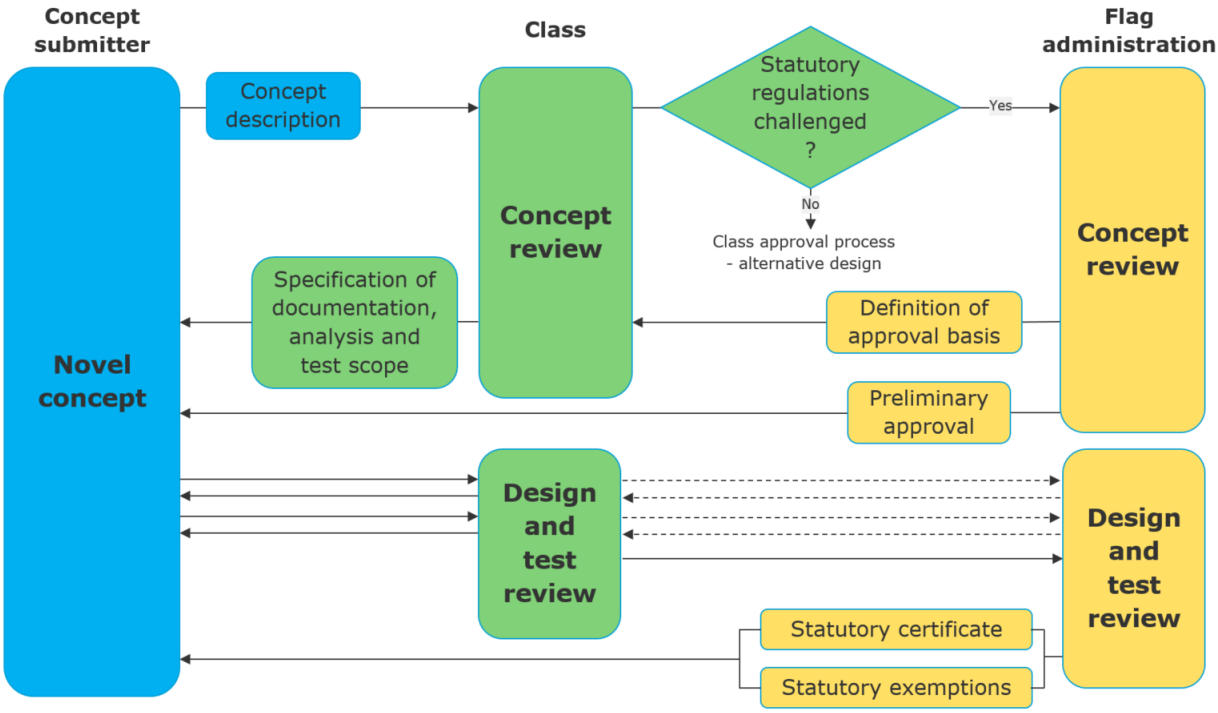


**Figure 3 The interactions between concept submitter, class and flag administration**

## 2.2 Process overview

As described earlier, this guideline is based on the assumption that DNV GL takes on a role between the concept submitter and the flag administration in documenting equivalence and obtaining approval of a new operational concept. For DNV GL to take on this role it is recommended that the vessel is classed with DNV GL.

The process described below focuses on the process steps between the concept submitter and DNV GL as a coordinator, i.e the left part in Figure 3. The level of engagement by the flag administration in the different steps, in particular the design and test reviews, will be subject to clarification between the respective flag administration and DNV GL for each project and is not addressed in this guideline.

An overview of the interaction between the concept submitter and DNV GL is illustrated in Figure 4, and the different activities are described in the subsections [2.3] to [2.8].

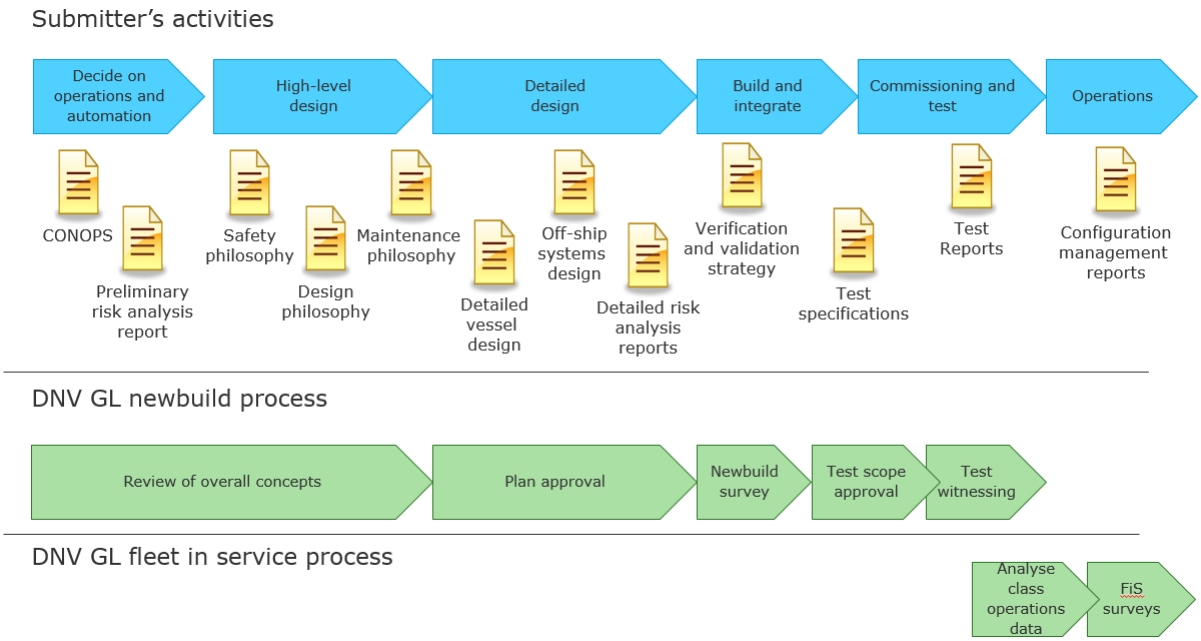


**Figure 4 Interactions between the submitter and DNV GL for concept qualification**

## 2.3 Decide on operations and automation

### 2.3.1 Concept of operation

The first step is for the submitter to decide on which of the operational tasks that traditionally have been performed by crew that will be performed either by remote-control and/or automatically.

In some cases, the project's goal is to reduce or remove crew from the vessel (compared with conventional ship operations). In other cases, the goal is not to reduce the crew, but to increase the safety or efficiency of the operations with the current crew.

The concept of operations should clearly describe all the operational tasks that the vessel will undertake that will be either fully or partly automated.

Each operational task should be further broken down into sub-tasks to a level that enables a clear distinction between tasks where a human is in charge of decision making and tasks where a system is in charge of decision making.

When a human is in charge of decision making, the location of the decision maker should be clearly described. Typically, this will be either:

— on-board
— from a remote control centre (RCC)
— a combination of persons on-board and persons in a RCC.

Whenever human intervention is expected or required by the system(s), special attention should be placed on the timing aspects, and the ability of the human to establish sufficient situational awareness so that correct actions can be taken within reasonable time (this is sometimes referred to as the command latency).

Other aspects of the planned characteristics and operations should also be described, including, but not limited to:

— operational area(s)
— vessel characteristics
— jurisdictions and regulations
— safety and availability targets
— weather and sea-state limitations
— presence of crew or other personnel on board the vessel
— roles and responsibilities of involved personnel
— minimum risk conditions for the vessel
— remote control centre characteristics
— communication-link characteristics (including coverage analysis of wireless communications)
— preliminary performance requirements for the key autoremote functions and systems (e.g. safe speed, vessel not under command, position keeping, object detection ranges, object identification, etc).

Such description of operational aspects should be contained in the document concept of operation (CONOPS). To aid customers in creating good CONOPS documents, DNV GL provides a CONOPS template as well as lists of possible modes, operations and tasks typically relevant for commercial vessels, and may be subject to automation and remote-control. These documents can be obtained upon request to the DNV GL.

### 2.3.2 Preliminary risk analysis

After (or in parallel with) the definition of operational aspects, risks associated with the proposed operations need to be identified and managed.

A preliminary risk analysis should be performed using a recognized method. The purpose of this is to determine critical risks that need to be mitigated by new or updated operations and/or tasks. The CONOPS should be updated to reflect the results of the risk analysis to ensure that all reasonably foreseeable events are covered.

As a minimum the preliminary risk analysis should cover the relevant hazards/failures/situations described in the following chapters:

— navigational functions, see Sec.4 [1.2]
— vessel's engineering functions, see Sec.5 [3]
— remote operations, see Sec.6 [3.1]
— communication aspects, see Sec.7 [2].

The risk analysis should include risks towards humans, the environment, the vessel itself, its cargo, and related off-ship systems.

The output from the preliminary hazard analysis may result in changes to the CONOPS; typical risk-mitigation activities including addition or removal of operations or tasks, redefined MRCs, addition of autoremote functionality, or adding operational constraints, e.g. with regards to sea and visibility conditions.

All required risk-mitigation actions should be identified, planned, executed and tracked to completion with clear traceability.

The CONOPS and the risk analysis is typically iterated until all relevant risks are managed.

### 2.3.3 Documentation

— concept of operation (CONOPS), to be sent to DNV GL for information
— high level risk analysis report, to be sent to DNV GL for approval.

## 2.4 High level design

The high level design phase aims at making the overall design decisions for the autoremote infrastructure. The main objective at this stage is to make sure the design can fulfil operational requirements and at the same time maintain required safety level and that the systems are maintainable.

The high level design balances aspects of functionality, performance, availability, safety and maintainability. Major design decisions like propulsion arrangement, fire-fighting capabilities and system architecture should typically be made at this stage.

This design serves as a basis for discussions with potential system providers, and should be updated based on the input from suppliers regarding specific system capabilities.

During the high level design phase, it should be investigated to what degree the technology planned used is novel or conventional. Novel technology should be qualified through technology qualification process (see [4]) while conventional technology should follow normal product certification process (see [3]).

An approval in principle (AiP) will normally be issued by the Society for novel technology that has gone through technology qualification. The AiP typically contains a list of aspects that have not been possible to verify, and thus needs to be verified during the concept qualification process.

Potential system providers should provide evidence of to what degree their system and its functionality is conventional and proven.

As a minimum, the output from the conceptual design phase should cover safety, maintenance and overall design aspects of the vessel, either as chapters in a combined document, or as separate documents, below referred to as philosophies.

### 2.4.1 Safety philosophy

The safety philosophy describes how the safety level of the vessel will be achieved. Depending of the scope and intent of the concept intended qualified, content of the safety philosophy may vary, but it should cover all relevant safety aspects as it is a key document when it comes to the administration's approval of the concept.

The safety philosophy should at least detail the following aspects:

Exemptions from current rules: a novel concept often challenge some of the existing rules put in place by the flag administration. An analysis should be performed towards the existing rules, and the gaps clearly identified. Alternative solutions may be outlined, and in some cases this results in requirements on the involved systems. In some case there will be need for focussed risk analysis in order to clarify that the proposed, alternative solution will result in an equivalent safety level.

Minimum risk conditions: minimum risk conditions (MRC) outlined in the CONOPS should be detailed, and when applicable, structured into hierarchies with clear priorities and decision trees. The same MRCs may be structured in different decision trees for different scenarios. The MRCs which serve as the last resort indecision trees should be clearly indicated.

Manning and competency: humans are typically a key and integral part of any safety system. The formal and informal requirements regarding competency for the humans involved with the operation and maintenance of an autoremote vessel should be described. Care should be taken to incorporate special competency needs related to remote supervision and control of the vessel operations.

### 2.4.2 Overall design philosophy

The intention with the design philosophy document is to describe how the autoremote infrastructure of the vessel will be designed to meet criteria resulting from CONOPS, risk assessments and safety philosophy.

The design philosophy should describe the overall design decisions, requirements and constraints for the systems intended for implementing autoremote functions. The document should describe redundancy and fault tolerance for the systems in order to ensure the capability to enter and maintain MRC in any scenario.

As a specific autoremote function may be implemented with systems from different suppliers, it is important that the design philosophy defines the boundaries of each system.

In order to determine the level of qualification and verification needed, the design philosophy should point out the maturity of each system, interface and related functionality with regard to intended use, and categorize the systems into following categories:

— type approved systems intended used in conventional application
— type approved systems intended used in new application or serving new purpose
— conventional system (without type approval) intended used in conventional application
— conventional system (without type approval) intended used in new application or serving new purpose
— system holding an approval in principle after having been through technology qualification
— systems that shall go through technology qualification.

### 2.4.3 Overall maintenance philosophy

The introduction of autonomous and remotely controlled systems may imply reduction in the number of required personnel in the vicinity of the systems and machinery. Therefore, special attention should be paid to maintenance of systems implementing autoremote functions. The maintenance philosophy should outline how each system will be monitored, diagnosed, maintained and repaired. Both software and mechanical sub-systems/components should be included in the analysis. The responsibilities of the different roles, both on board the vessel and onshore should be clearly defined.

### 2.4.4 Documentation

Safety philosophy, design philosophy, maintenance philosophy (may be combined into one document), to be sent to DNV GL for information.

## 2.5 Detailed design

The detailed design phase is where design decisions regarding the vessel are made. For autoremote functions, focus of this phase is to make sure that each system will be able to provide desired autoremote functionalities and that interfaces between different systems are sufficiently defined. Combinedd, the vessel design documentation and the off-ship systems design documentaiton describe the total infrastructure needed to safely implement autoremote functions.

The complete autoremote infrastructure is shown in Figure 5.

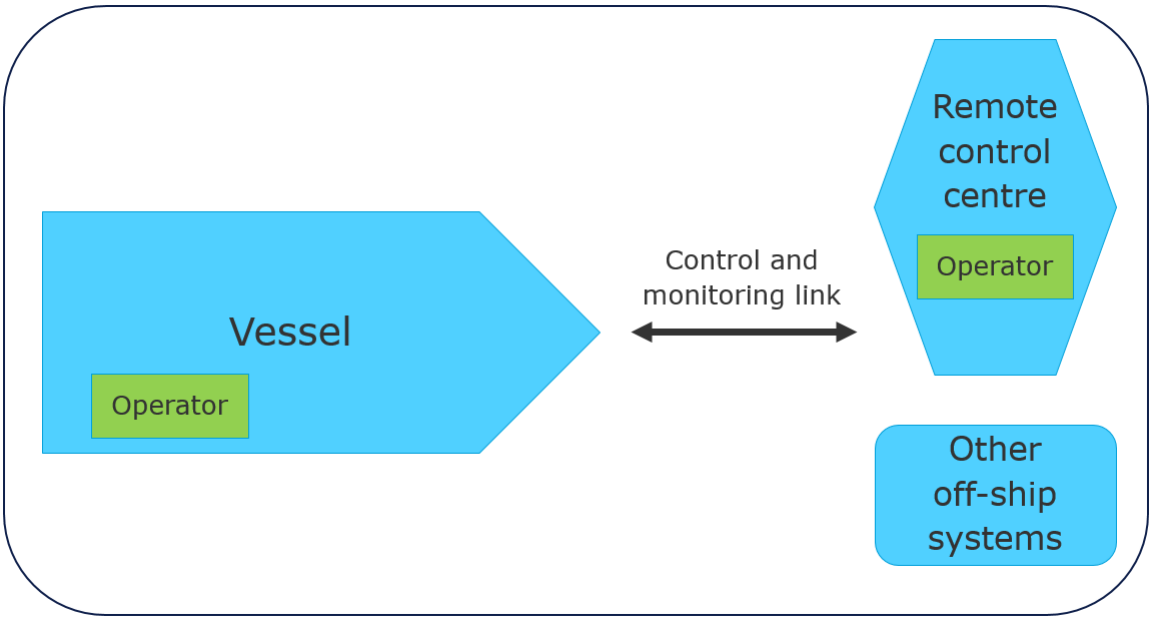


**Figure 5 Autoremote infrastructure**

### 2.5.1 Vessel design

Vessel design documentation should in addition to the conventional content, also specify special arrangements needed to fulfil requirements on autoremote functionality and systems.

### 2.5.2 Off-ship design

Off-ship systems design documentation defines infrastructures needed off the vessel in order to safely implement autoremote functions. It typically contains design documentation for a remote control centre and off-ship part of communication link(s) connecting the vessel to the remote control centre. Also, other off-ship systems, e.g. for object detection, towing and mooring should be included.

### 2.5.3 Detailed risk analysis

A detailed risk analysis of autoremote systems in total should be performed on basis of CONOPS, safety philosophy, design philosophy, off-ship systems design and vessel design information. The purpose is to ensure that the autoremote infrastructure as a whole is able to deal with relevant failures and situations in safe manner.

The risk analysis should be performed using one or more established risk analysis methods such as fault tree analysis (FTA), event tree analysis (ETA) or failure mode and effects analysis (FMEA).

Functions and systems for autoremote functionality are expected to be able to handle a number of failure modes. Some of the situations and failure modes may be project specific. In addition, the technical guidance sections in this guideline lists a number of hazards, incidents and failure modes with expected responses that should be taken into consideration in the detailed risk analysis.

If the the operational concept includes remote operations from a remote control centre, this should be analysed through a separate risk analysis. A risk analysis method focusing on human aspects should be used for this purpose. Examples of such methods are crisis intervention and operations analysis (CRIOP) and operating and support hazard analysis (O&SHA).

All identified risk mitigation actions from risk analysis activities should be planned, executed and tracked to completion. The mitigating actions should be traceable.

The risk analysis should show the level of risks associated with intended autoremote functions as they shall be implemented.

### 2.5.4 Documentation

— vessel detailed design documentation, to be sent to DNV GL for approval
— off-ship systems design documentation, to be sent to DNV GL for approval
— detailed risk analysis reports, to be sent to DNV GL for approval.

## 2.6 Build and integrate

The build and integrate phase involve several activities, but this guideline focuses mainly on the scope and thoroughness of verification and validation, because this are key parts of technology qualification.

Verification and validation strategies should be made up of several different inspections, reviews, test-types and test-environments. Because it is (almost) impossible to test all aspects of a complex system, it is important to also utilize other verification methods like review and analysis.

The verification activities should seek to prove that the system fulfils the specifications and requirements, while the validation activities seeks to prove that the system is fit for purpose compared with its intended use.

A comprehensive verification and validation (VV) strategy is expected to be produced at this stage, describing how functionalities regarding autonomy and remote operations of the vessel will be verified before they are used operationally. The VV strategy should describe reviews, test-stages, test-types and test-environments that autoremote functions shall pass before final acceptance.

For each VV-activity, purpose, scope and responsibilities should be described. For each test-stage, test-environment, its capabilities and limitations should also be described.

For a concept qualification project to succeed is it important that the acceptable performance of an autoremote infrastructure is defined, and that the different VV activities seek to verify the actual performance of the total system.

VV strategies should consider that systems having already obtained approval in principle, may still need validation in real operational environment.

See [4.3.5] for a description of some test types and test environments that may be utilized, including simulators.

The VV strategy should not be confused with a detailed test specification/procedure or test-plan describing test-cases.

### 2.6.1 Documentation

Verification and validation strategy, to be sent to DNV GL for approval.

## 2.7 Commissioning and testing

### 2.7.1 General

The commissioning and testing phase focuses on creating and executing sub-system and system-wide tests in accordance with VV strategy to provide evidence that the total autoremote infrastructure and its individual systems are behaving as expected.

### 2.7.2 Test preparation

Test specifications should be prepared. These should include a detailed description of the test-cases that will be run during the site acceptance tests/on-board tests of the autoremote functions.

The test procedures/specifications should include detailed information of the system intended tested including system type, hardware identification and software versions. Any simulators used in the test setup shall also be described and recorded with type and version.

For redundant systems, a selection of tests within each system analysed in the FMEA should be carried out. Specific conclusions of the FMEA for the different systems should be verified by tests when redundancy, fail safe response, or independency is required. The test selection should cover all specified technical system configurations.

Test procedures for redundancy should be performed under as realistic conditions as practicable, e.g. by use of simulators.

Test scope should be divided into 3 categories of tests:

— functional testing : testing ensuring that system functions are working as intended and according to technical and operational descriptions.
— performance testing : testing of a system's capability to perform its intended functionality. Responsiveness, stability and reliability are important aspects that should be included.
— failure response testing : testing of failure modes to ensure that the system is handling failures safely and according to rules and given standards, and that redundancy principles are maintained after failures. Test cases should be performed in different environmental conditions (simulated) and in different operation modes and vessel setting.

All tests cases should describe the purpose, description and expected results.

### 2.7.3 Test execution

Each time a test-case is run, results should be recorded along with any discrepancies toward the expected results.

A test evaluation should take place in order to verify that the ambitions of the verification and validation strategy are met.

### 2.7.4 Documentation

— test reports, to be sent to DNV GL for information
— overview of failures, to be sent to DNV GL for information
— test evaluation report, to be sent to DNV GL for approval.

## 2.8 Operations

### 2.8.1 Data collection and analysis

In order for DNV GL to develop future survey schemes, and in order to improve on technical guidance and rules, data from the operation of the autoremote functions should be collected and analysed and made available to DNV GL as agreed with the owner and operator of the vessel. Typically, the data include aspects like hours of operations, detected failures, entering and leaving MRCs, and other operational data used for condition monitoring. Details regarding data collection, processing and storing, e.g. data model, collection methods, frequency etc. will be determined per vessel with relevant stakeholders.

### 2.8.2 Vessel surveys

Any vessel in operation is subject to a survey scheme where the conditions and capabilities of the vessel is inspected and verified for compliance with applicable rules and regulations. For autonomous and remotely operated vessels no such survey scheme is yet established in the industry.

It is foreseen that the starting point for the new survey scheme will be today's class systematics, i.e. primarily a scheme of annual, intermediate and renewal surveys - in addition to follow-up and possible surveys following incidents or damage and eventual changes and modifications to the systems. However, the autoremote vessel s will necessarily utilize new technological solutions to a wide extent, and many of the systems may neither be adequately nor efficiently surveyed via the traditional methods. New ways of verification/surveys that are currently being developed may supplement or substitute parts of this scheme - where an equivalent or better level of verification may be provided e.g. by new digital solutions.

The main intention of the in-service surveys is to confirm that the hull, machinery, equipment and systems remain in satisfactory condition and in compliance with applicable rules and regulations - to uphold the certificates.

Since the scope of the surveys cover a wide range of aspects spread from mechanical properties of the hull, tanks, coatings etc. to the various properties of integrated machinery systems, the impact of the new, autoremote capabilities of the vessel differ widely for the various survey items.

It is therefore expected that a certain part of the survey scope covering physical, mechanical properties of the vessel will mainly be based on the traditional methods of survey, unless substituted - or supplemented - e.g. by more sophisticated condition monitoring capabilities.

When it comes to the parts of the survey scope covering the more SW intensive autoremote functionality where the systems may be based on novel technology, other validation and verification methods may be utilized. This implies that the surveys will be more flexible including new elements, i.a. to strengthen / allow for the following aspects:

- Utilize the new possibilities enabled by i.a. digitalization and connectivity, e.g. remote surveys, simulator testing, built-in test capabilities.
- Less calendar-based surveys, more based on the above aspects for reporting, monitoring and other appropriate verification methods, risk based surveys.
- Condition monitoring, where physical presence and at-site inspections may be supplemented or substituted, less intrusive inspections.
- SW change management, in particular a structured SW change management process. SW changes may for certain systems/functions necessitate rigorous testing and simulation at different steps in the process, including also regression tests.
- Cyber security aspects is essential and must be duly addressed.
- The operational aspects largely depend on an remote control centre (RCC), and the survey scheme will probably include both the technical and organisational properties of the RCC including the means of communication.

The first projects will probably entail a stepwise transition from manually operated functions to more remote or autonomous operation over a period of time in operation, where the different functions of the vessel are gradually qualified for remote or autonomous operation. Each such step will have to be planned for, implemented, verified and surveyed to uphold the vessel certificates.

Since a vessel with any degree of autonomy affect the operational organization, -responsibilities and -decision process, the safety management system will be affected. It is foreseen that the operators safety management system will be subject to audits based on elements from the ISM scheme.

DNV GL plans to publish a separate guide for remote operation centres in the future.

The scope of the management system audits and the split towards the in operation survey scheme will be part of the development.

### 2.8.3 Change management of Software

DNV GL shall be notified of any changes to the target system including software and the documentation in accordance with DNVGL-RU-SHIP Pt.4 Ch.9 Sec.1 [1.5]. The notification should contain the reason for change and the impact on the target system and the operational philosophy.

An autoremote vessel will be highly dependent on software (SW) and the key functions rely on software intensive systems. Management of changes, software changes in particular, in the operational phase will become even more important than for a conventional vessel - in order to ensure the safety and availability of the key functions.

This necessitate a structured SW change management process and strict adherence to the defined SW change management procedures.

The general class approach for SW change management in control systems in the operational phase is illustrated in the simplified process below (see Figure 6); the main principles are as follows:

- All SW changes shall be handled in a structured way containing at least the different steps as shown in the illustration in Figure 6.
- The change management process shall be formalized in an official procedure/instruction.
- To ensure traceability, all changes shall be recorded in a log where necessary evidence document that the principles of the procedure has been applied.

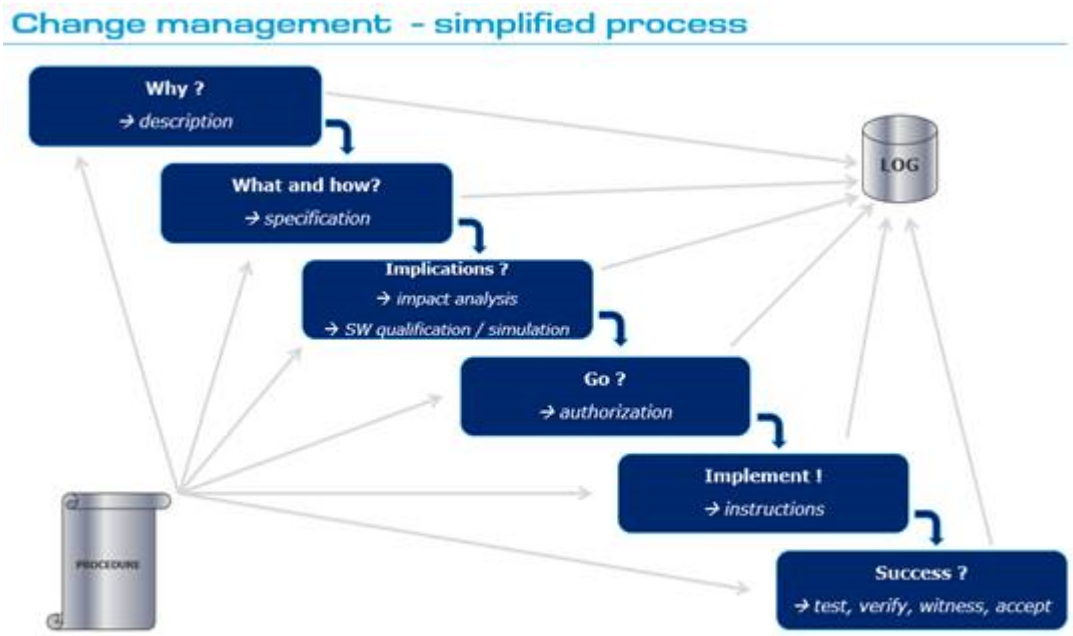


**Figure 6 Simplified change management process**

For autoremote vessels, it is foreseen that certain steps in this general process will have to be enhanced with more thorough and elaborate verification, i.e by the use of more simulator based testing and regression tests, i.a. prior to - or in connection with the actual implementation on the target systems on board or in the RCC.

The cyber security aspects, both in relation to the process of upgrading the systems as well as maintaining the integrity of the cyber security properties in the involved IT and OT systems is an essential element in the SW change management process.

# 3 Approval of conventional technology

## 3.1 General

Conventional technology to be used in conventional ways are approved by DNV GL trough standard procedures for type approval and product certification. This guide only contains a general overview of the process for the sake of completeness.

## 3.2 Process overview

For technologies of conventional design where performance requirements to the technology already exists and the performance is sufficient to support new operational concepts, the general class process for approval of products applies.

An overview of the approval process for conventional products is depicted in Figure 7.

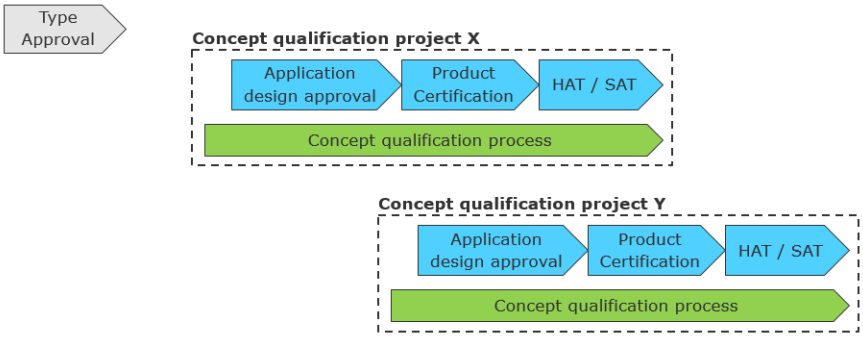


**Figure 7 Approval process for conventional products**

The general process for approval of conventional products is described in DNVGL-RU-SHIP Pt.1 Ch.1 Sec.4. The following is a summary of the main elements shown in Figure 7:

— type approval (TA)

  Mandatory scope of TA is verification of compliance with the marine environmental specifications. TA may also cover performance and test requirements to the functionality if the functionality is not application dependent for the specific use on-board a vessel. Verification of cyber security capabilities is also offered by dedicated TA.

  TA covers verification of standard fixed features of a system or component, and will in this way reduce the design approval and test scope for each delivery.

— application design approval

  Case by case verification and approval of a system or component for use on board a specific vessel. The manufacturer should document how application dependent features of a system or component is designed for compliance with the relevant requirements.

  The documentation requirements include, among others, a functional description and a test program to be used in the product certification test (should cover testing of normal functionality and failure modes). Application design approval is also referred to as plan approval in DNV GL rules and is mandatory for product certification.

— product certification test

  The purpose of the product certification test (often referred to as factory acceptance test (FAT) in the industry) is to demonstrate by testing that the product performs according to the approved application design with respect to normal functionality and response to failures.

  The product certification test is carried out at the premises of the manufacturer before the product is shipped for installation on board the vessel. A product certificate will be issued by DNV GL as documentation to the newbuilding project that the product is in conformance with the required functionality applicable for the intended use on board the vessel.

— on board tests

  After installation of the product on board the vessel, the product will be subject to integration testing towards other systems and components. The product functionality will be subject to final verification as part of the vessel's harbour tests and sea trials.

# 4 Technology qualification process

## 4.1 General

This subsection provides a description of the process to follow for manufacturers of novel technology supporting the new operational concepts described in [2].

DNV GL class rules open for acceptance of novel technology:

— DNVGL-RU-SHIP Pt.1 Ch.1 Sec.1 [2.5.9]: *Alternatives to detailed requirements in the Rules may be accepted when the overall safety and reliability level is found to be equivalent or better than that of the Rules.*

— DNVGL-RU-SHIP Pt.1 Ch.1 Sec.1 [2.5.10]: *If detailed requirements are not prescribed in the Rules, the Society may consider the safety and reliability level of a proposed solution, or require clarification to resolve the issue.*

Novel technology for which performance requirements have not been developed should follow the qualification process described in this section.

If a conventional technology (e.g. a radar) is intended used to enable a new operational concept where the existing performance requirements to the technology are not sufficient to support the new operational concept, the qualification process described in this section should be followed.

## 4.2 Process overview

This subsection provides a description of the process to follow for novel technology supporting autonomous and remote control of vessel functions.

An overall illustration of the process for class approval of novel technology is shown in Figure 8.

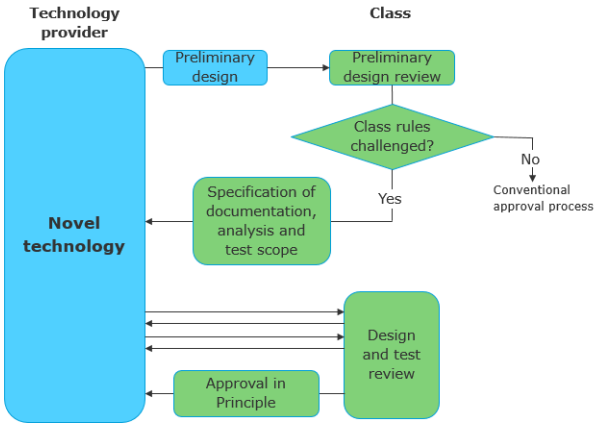


**Figure 8 Process for class approval of novel technology**

The overall process is similar to the concept qualification process described in [2]. However, as can be seen from above Figure 8, the flag administration is not involved in the technical qualification of novel technology since the technology by itself does not challenge any statutory regulations. When the technology is used in new operational concepts challenging statutory regulations (e.g. with the purpose to remove crew from the vessel), use of the verified features provided by the technology to achieve an equivalent level of safety for the new operational concept will be subject to approval by the flag administration as described in [2].

The approval process for novel technology includes the same main elements as the approval process for conventional products described in [3] (i.e. type approval, application design approval, product certification and on board tests), but with additional elements addressing the novel features provided by the technology.

Technology qualification may be carried out in two ways:

— approval in principle (AiP)

Intended for manufacturers that have developed a product with novel features, where the novel features are sought documented and verified before presented to industry for possible use in different concept applications. The AiP will specify verified performance capabilities of the product, enabling concept developers to consider use of the technology for their concepts. This is illustrated in Figure 9.

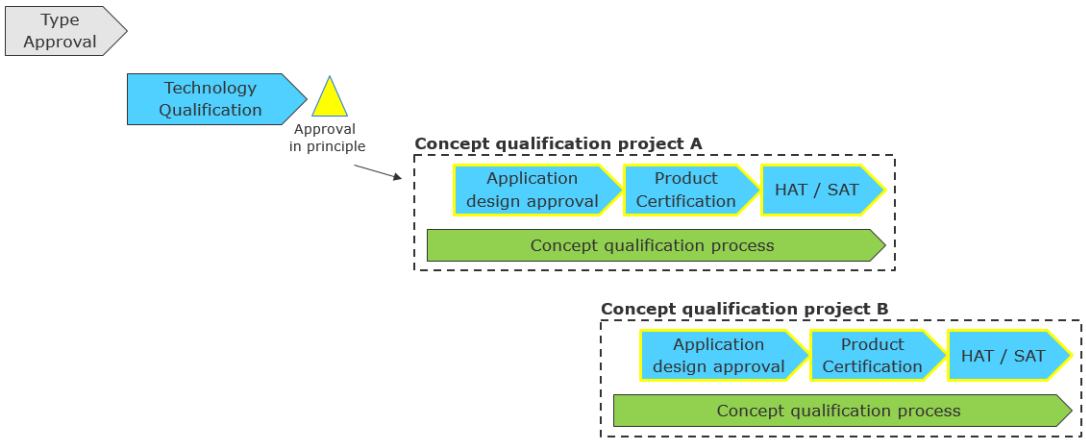


**Figure 9 Approval in principle, standalone TQ**

— concept specific technology qualification

Intended for manufacturers engaged to provide technology to a specific new operational concept, where the needed technology performance will result from the concept development process. Verification of technology performance will be carried out as an integral part of the concept project, as illustrated in Figure 10.

Performance verification in the concept project may be used as part of the basis for obtaining an approval in principle for use of the technology in other concepts.

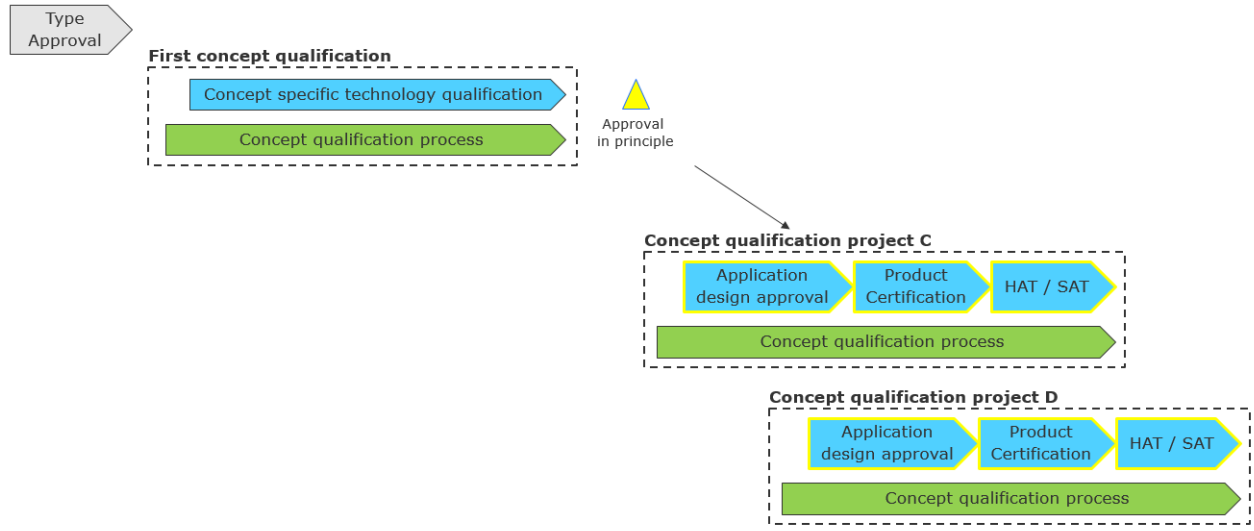


**Figure 10 Concept specific technology qualification**

## 4.3 Process guidance

DNVGL-RP-A203 provides a recommended practise for technology qualification. The different steps of the recommended technical qualification process are shown in Figure 11.

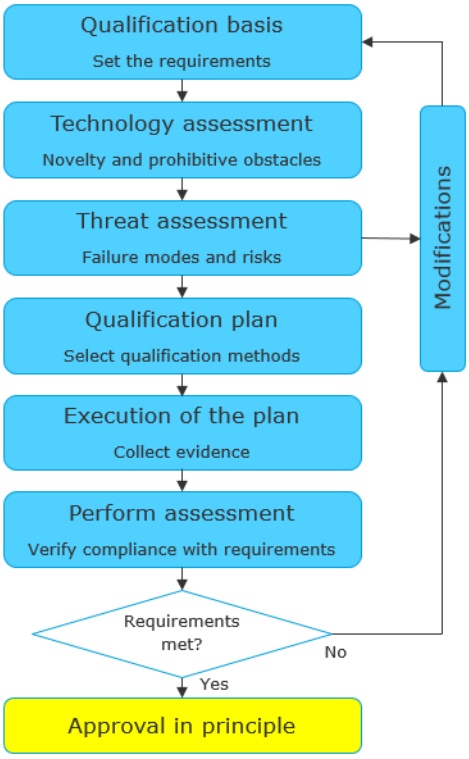


**Figure 11 The generic technology qualification process**

This guideline follows the principles of the technology qualification process described in DNVGL-RP-A203 and gives in the following sub-sections further guidance to the steps in this process with respect to qualification of technology related to systems supporting autonomous and remote control of vessel functions.

For autonomous and remote operations, much of the novel technology will rely on software, and thus the technology qualification process described in this guide includes guidance regarding technology qualification of software intensive systems (from DNVGL-RP-A203 App.D).

The generic technology qualification process has been tailored to the use in the context of autonomous and remotely operated ships, resulting in the process illustrated in Figure 12.

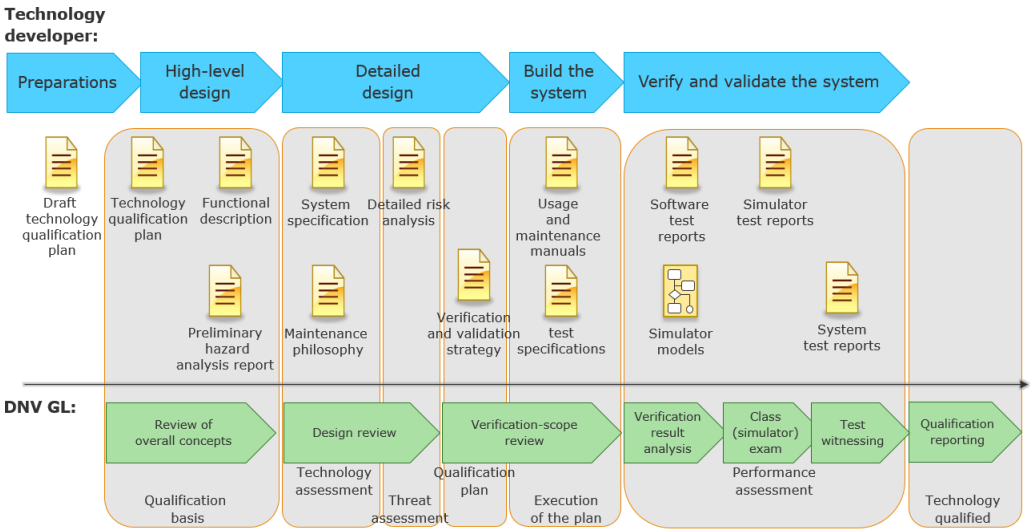


**Figure 12 Process interactions between the technology developer and DNV GL for technology qualification**

### 4.3.1 Preparations

During the preparation phase the technology qualification is planned and the requirements for the technology qualification are outlined, both regarding technical requirements, process requirements and DNV GL's involvement.

It should also be determined if the technology qualification will be performed as a stand-along project (e.g. by a technology developer), or if it is to be performed as a part of a concept qualification process (see [2]).

Ideally, DNV GL is involved in the project from this early stage, but it is also possible to apply the technology qualification process even if the technology (or product) development has already progressed ahead. In such case, some of the activities described here can be performed retroactively or, if they were performed at an earlier stage, the resulting documentation or evidence can be provided to DNV GL.

If the technology (or product) to be qualified relies on software as a part of the main or critical functionality, the software development life-cycle should be decided up-front.

#### 4.3.1.1 Define the software life-cycle (if applicable)

Verified system & software development and configuration processes should be used to create and deliver the functionality in question.

The verification of the processes in question can be done by submitting proof that an independent party has verified the content and the application of the processes.

The technology developer can choose between several available standards e.g.:

— DNVGL-CP-0507 *System and software engineering*
— ISO/IEC 12207 *Systems and Software engineering - Software life-cycle processes*
— ISO/IEC 15288 *Systems and Software engineering - System life-cycle processes* .

The verification of the processes in question can be done by submitting proof that an independent party has verified the content and the application of the processes.

The defined ways of working (process) for the software development and configuration should be included in, or referenced from the Technology qualification document.

#### 4.3.1.2 Documentation

Draft technology qualification plan, to be sent to DNV GL for approval.

### 4.3.2 High level design

The next step in the process is to establish a qualification basis identifying the technology, its functions, its intended use, as well as the expectations to the technology and the qualification targets. This activity is similar to the initial step in the concept qualification process of establishing a CONOPS. The focus is however not on a vessel operation level, but on a functional level of the system in question. Use-cases may be used to capture the intended interaction between the system and its users.

#### 4.3.2.1 Define the functionality of the system

In order to define the required functionality, a functional description document should be established where the following is described:

1) Normal operation

   A description of how the function works and behave under normal conditions. If applicable, the functionality may be divided into several sub-functions. For examples of potential functions, see App.B.

2) Autonomy and remote control modes

   A description of how the function behaves in different modes with regards to decision support, autonomy and remote control. The expected human interaction should be described, and how the function behaves if expected/required human input or intervention is not available (e.g. due to a communications failure with the remote-control centre).

3) Sequences and timing

   Automated sequences and timing aspects of the functionality should be described. If the system is expecting input from a remote operator, there should normally by a time-out action which prevents the function from 'hanging' if the input does not happen as expected.

4) Man-machine interfaces

   The interface between the system and the human users shall be designed according to best practises for user interfaces and with defined responsibility modes for the operator. Especially situations where a human is expected to 'take over' control because of system-limitations or failures should be designed to allow ample time for the human to get the required situational awareness in order to be able to make good decisions (this is sometimes referred to as the control latency).

5) Degraded/limited functionality

   A description on how the function behave when it is not able to operate at 100%. The characteristics of the degraded/limited functionality should be described along with the consequences of the limitation(s). Loss of redundancy should be regarded as a degraded mode.

6) Safe state(s)

   A description of the state(s) the function is going to end up in the event of a failure. For guidance to the expected result of different failure categories, please see Sec.5 [3.1.3]. The function should be designed so that the safe-states are predictable and controllable.

#### 4.3.2.2 Identify relevant, already established acceptance criteria

Products to be installed on board vessels are subject to general requirements that will apply for a product irrespective of the function the technology is intended to provide. Examples of such requirements are:

— the product shall be suitable for installation in a marine environment
— general requirements to HMI, such as e.g. alert management
— self-monitoring capabilities
— compatible communication interfaces.

The above list is not exhaustive. Relevant applicable requirements are given in various parts of the classification rules and statutory regulations. A complete list of existing classification and statutory requirements applicable to the product should be established for each technology qualification project.

#### 4.3.2.3 Define performance specifications

The technology developer specifies the expected performance of the technology for certain defined parameters. The scope of the AiP will be to verify performance in accordance with the specifications.

Relevant performance parameters for some types of technologies and functions are given in Sec.4 to Sec.7 of this guideline. The intention is to extend this in the next editions of this guideline to provide relevant performance parameters for all the typical technologies used to enable autonomous and remote control of vessel functions.

For the software components of a system, the ISO/IEC 25000 series of standards give valuable input for defining performance parameters. In particular ISO/IEC 25010 gives information about potential characteristics (quality attributes) for a software component, covering characteristics both the software itself and the use of software.

If a technology developer presents a technology for which no performance parameters have been defined, DNV GL may case-by-case define the relevant performance parameters for the technology to be applied for the specific AiP, as well as updating the subsequent edition of this guideline with parameters for the type of technology.

#### 4.3.2.4 Preliminary hazard analysis based on the functional description

The functionality described in the functional description should be analysed to identify risks based on the intended use as described in the CONOPS document. Recognized HAZID methods should be used. The HAZID analysis may lead to changes in the functional description or put requirements on the design of the system(s) in question.

Required risk-mitigation actions should be clearly identified and tracked to conclusion.

#### 4.3.2.5 Documentation

— Functional description; to be sent to DNV GL for information.
— Technology qualification plan including a definition of the verification basis; to be sent to DNV GL for information.
— Preliminary hazard analysis report; to be sent to DNV GL for approval.

### 4.3.3 Detailed design

The next step in the process is to detail the system design and at the same time assess the technology by categorizing the degree of novelty to focus the effort where the related uncertainty is most significant and identify the key challenges and uncertainties.

The technology qualification basis described in the previous subsection forms the input to the technology assessment.

#### 4.3.3.1 Technology composition analysis

The objective of the technology composition analysis is to describe the novel elements of a compound technology. This is a top-down assessment that starts with the system-level functions and proceeds with decomposing the technology into elements including interfaces.

The decomposition should result in a description of:

— system description
— system topology
— functions and sub-functions with further sub-division as required, without reference to the technical solutions used to deliver the functions
— sub-systems and components with functions
— interface descriptions
— operational sequences.

For complex systems, a system engineering approach is recommended using a hierarchical structure linking the technology expectations (goals) to functions and sub-functions. At the appropriate level, sub-functions are delegated to hardware or software components.

If the system contains sub-systems, there may be a hierarchy of documents to completely describe the whole system in question.

How to perform maintenance of the system should also be described at this point.

The maintenance plan for the system describes how maintenance is supposed to be performed. This is especially important in the case of autonomous and remote operated functionality, where there may be limited human availability for maintenance tasks.

For software systems, the maintenance plan should at least describe how the software and relevant data are to be updated, backed-up and restored.

#### 4.3.3.2 Technology categorization

Novel technologies typically evolve from existing proven technologies. Normally only some elements of the technology are novel. Uncertainty is associated mainly with the novel elements. In order to focus on where uncertainty is greatest, the novelty categorizations in Table 1 can be used.

Both the novelty of the technology itself and its application area affect the uncertainty associated with the technology. Elements categorized as novel (category 2, 3 and 4) should be taken forward to the next step of technology qualification for further assessment.

Regarding software: new software should be categorized as novel or unproven, and substantially modified software should be categorized as limited field history. Each software component should be considered separately. Thus, some software components may require qualification, while others do not.

Only knowledge and experience that is documented, traceable and accessible to the qualification team should be used to reduce the degree of novelty.

**Table 1 Technology categorization**

| | *Degree of novelty of technology:* | | |
|---|---|---|---|
| Application area: | Proven | Limited field history | New or unproven |
| Known | 1 | 2 | 3 |
| Limited | 2 | 3 | 4 |
| New | 3 | 4 | 4 |

This categorization indicates the following:

1) no new technical uncertainties (proven technology)
2) new technical uncertainties
3) new technical challenges
4) demanding new technical challenges.

The categorization in Table 1 may not be suitable for all technologies. This may be related to challenges in defining what should be considered as known or proven and the relevance of the past experience. An alternative approach to categorize the technology is given in Table 2. This approach is focusing on the existence of acceptance criteria rather than a subjective assessment of the novelty of the technology. It is also based on an assessment whether the limits to operation are known rather than a subjective assessment of the novelty of the application area.

**Table 2 Alternative technology categorization**

| | *Limits to operation:* | | | |
|---|---|---|---|---|
| Acceptance criteria for delivery: | Not applicable | Quantified | Unquantified (method defined) | Undefined method |
| Not applicable | 1 | 1 | 2 | 3 |
| Quantified | 1 | 1 | 2 | 3 |
| Unquantified (method defined) | 2 | 2 | 3 | 4 |

| | *Limits to operation:* | | | |
|---|---|---|---|---|
| Undefined method | 3 | 3 | 4 | 4 |

The method considered most suitable and accordingly chosen for a specific technology should be argued for and agreed with DNV GL.

#### 4.3.3.3 Detailed risk analysis

The next step in the process is to assess threats and identify failure modes and their risks.

The detailed risk analysis of the system should show how the system design maintains the functionality in question and keeps the risks to life, environment and property equivalent to (as safe or safer) current conventional solutions. Recognized risk analysis methods like FTA, ETA, and FMEA should be used. More than one analysis method may be necessary to fully analyse the risks.

In order to make the quantification of the risks feasible, it is recommended that the probability categories are limited to three in this analysis:

— Failure is not expected (i.e. exempted).
— Failure may be expected within the lifetime of the product/vessel (i.e. potential failure).
— Failure may be expected several times a year for a product (i.e. anticipated failure).

Below is a description of one of the most used risk-analysis methods;

Failure mode and effect analysis

The main purpose of the FMEA is normally to demonstrate that redundant systems are not degraded beyond acceptable performance criteria after a single failure. The FMEA report should consist of at least the following parts:

1) general system information
2) specification of acceptance criteria
3) specification of the overall boundary of the system/unit subject to the FMEA
4) redundancy design intent, worst case failure design intent, time requirements, and the system's operational modes
5) specification of all redundant components and single component groups included within the overall system boundary. The relevant system names, main units, compartments (when applicable), and their main intended functions should be presented in a structured manner, supported with a descriptive narrative text
6) specification of all assumptions related to systems interfaces and dependencies of external systems
7) single failure and common cause analysis at unit and subsystem levels, including consequence for the function and eventual manual/automatic corrective actions assumed
8) summary and conclusions
9) a redundancy and failure mode test program specifying tests to verify assumptions and conclusions should be developed
10) a compliance statement referring to the overall system boundary, operational modes, tests, and acceptance criterion including time requirements should be stated for the FMEA.

The requirements to FMEAs for redundant systems differ from traditional, bottom-up FMEAs in the following:

— requirement to state the redundancy design intent
— requirements to specification of acceptance criterion to be complied with
— requirements to refer to full scale testing to support analysis
— requirements to state compliance with the acceptance criterion.

The FMEA documentation should be self-contained and provide sufficient information to get the necessary overview of the system.

Required risk-mitigation actions should be clearly identified and tracked to conclusion.

#### 4.3.3.4 Qualification planning

The next step in the process is to develop a plan containing the qualification activities necessary to address the identified risks. This document is refereed to both as a qualification plan and as 'verification and validation strategy' for the system in question. In addition to the verification and validation activities described in [4.3.5], the plan may include analysis and inspection activities.

The updated qualification plan should describe all the different verification and validation (VV) activities the function/system should go through before it is qualified. For each VV-activity the purpose, scope and responsibilities should be described. For each test-stage, the test-environment, it capabilities and limitations should also be described.

It is expected that software intensive systems are verified and validated using several different methods and test-environments.

#### 4.3.3.5 Documentation

— System description; to be sent to DNV GL for information.
— Maintenance plan to be sent to DNV GL for information.
— Technology qualification plan including technology analysis results ; to be sent to DNV GL for approval.
— Detailed risk analysis report(s); to be sent to DNV GL for approval.

### 4.3.4 Build the system

The next step in the process is to execute the activities specified in the technology qualification plan. Emphasis should be put on collecting evidence in the form of records from reviews, analysis and test activities.

It is also strongly suggested to keep a good trace between risks, requirements, design and test-cases on the different levels of the system in question.

Information about usage and installation of the system:

Information intended for personnel that install and use the system should be prepared early so that it can be verified against the actual system-behaviour during the verification and validation.

Preparation for tests:

In parallel with the actual building of the system, test cases for the verification and validation of the system should be prepared at this stage.

the tests may be divided into two groups:

1) in-house tests performed by the manufacturer
2) witnessed tests where DNV GL personnel observe the test execution.

Within both groups there may be several different test-activities and test-environments.

DNV GL expects that the manufacturer runs a comprehensive in-house test of the system, and the detailed test-coverage should be agreed per system.

The witnessed tests will typically only sample the complete test-scope. The scope of the witnessed test is going to be agreed per test activity.

#### 4.3.4.1 Documentation

— Operation manuals; to be sent to DNV GL for information.
— Internal test specifications; to be sent to DNV GL for information.
— External test specifications; to be sent to DNV GL for approval.

### 4.3.5 Verify and validate the system

The objective of verification and validation (VV) is to create genuine and trustworthy evidence with adequate quality. This requires the evidence to contain particular properties, which may be different to what is required in traditional test processes for previously qualified products. The next step in the process is to assess whether the evidence produced meets the requirements of the technology qualification basis.

The extended use of software for safety critical decisions and operations in novel technologies introduces new failure modes and requires new methods to test and verify the intended use and robustness of the code and algorithms. The use of simulator based technologies permits introduction of extended failure modes and sequence testing to cover the necessary scope of VV.

Using simulator technology to test and validate such systems are complimentary to requirements in DNVGL-RU-SHIP Pt.4 Ch.9 Sec.4.

Testing of complex software should not be limited to a few discrete, time-bound test activities. Instead, automated tests should be run frequently while the software is being developed.

As changes to software normally are easy to make (compared to hardware changes), the software is often updated several times during the verification and validation period. Care should be made to make sure that re-tests are executed when applicable, and that regression tests are run to verify that software updates to fix defects or to add functionality have not negatively affected previously verified functionality or capabilities.

#### 4.3.5.1 Simulator based testing

Safety critical functionality related to autoremote navigation should be prepared for the possibility of simulator based test setup according to defined interfaces (interfaces to be agreed with DNV GL).

Simulator based testing should provide objective evidence of suitable functionality (during normal, abnormal and degraded condition) of the specified target control system according to functional and safety requirements defined in the rules or originating from the detailed risk analysis.

Simulator based testing is especially useful for functionality where it is required to verify that the function (or whole system) will work satisfactorily in a large range of operational scenarios.

Examples of such functions are:

— voyage and route planning
— keep general lookout
— detection, tracking, classification of
  navigational dangers/objects and other vessels
— determine CPA/TCPA for navigational dangers/objects and other vessels
— determine the situational mode (e.g. unrestricted, dense traffic, costal navigation, narrow passage, restricted visibility, heavy weather, very cold weather, ice conditions, pilot required)
— grounding and collision avoidance
— weather routing.

The list above is not exhaustive. For other functions that potentially may be within scope for autoremote considerations, please see App.B.

Further guidance on simulator based testing is found in App.E.

#### 4.3.5.2 Redundancy and failure response tests

For redundant systems, a selection of tests within each system analysed in the FMEA should be carried out. Specific conclusions of the FMEA for the different systems should be verified by tests when redundancy, fail safe response, or independency is required. The test selection should cover all specified technical system configurations.

#### 4.3.5.3 Testing of integrated systems and functions

Integrated systems with high level of complexity and dependency should be subject to integration testing. Integrated solutions are subject to new emergent properties that need VV. Integration of such systems is normally done during commissioning and testing close to project completion. In some cases, this testing may be impossible due to the risk of damage to the system. Therefore, integration testing should be carefully planned and alternatives, such as simulation, should also be considered where appropriate.

The main objective of integration testing is VV of functions and dependencies between the systems that are critical for safe operations and prove that no emergent properties will degrade the systems.

Integrated testing could be done in a simulator environment using models and emulated or hardwired control systems. The scope of testing should also include critical failure modes (e.g. short circuit) that are challenging/impossible to perform on real HW.

#### 4.3.5.4 Factory acceptance test

The Factory acceptance test specification should describe the test-cases to be executed during the factory acceptance test. The factory test environment and scope should be in accordance with the VV strategy for the system. For each test case, the expected result should be defined.

In addition to the product certification test described in [3.2], the testing and validation specified in the FAT should be extended to include:

— control system software and algorithms
— emergent properties from integrated system of systems.

The HIL or SIL technology are well established methods for verifying the robustness of the software and opens the possibility of extended failure modes and scenario testing.

Software tests should be performed at an early stage. The objective of the software tests is to ensure that the control system SW is ready and verified as extensively as possible before the commissioning and sea trial period starts.

The technology developer is responsible for logging the versions of uploaded test target software. The target software should not be changed during a test activity unless it's imperative to continue the test activity. If such changes need to be done, the impact on the performed test cases will be analysed by DNV GL in cooperation with the technology developer. Invalidated test cases should be re-tested.

Test report from the factory acceptance test:

When all observations are categorized, a test result report should be issued for each product. This document will include all the observations found during testing, and should be updated throughout the project with:

— grading (including history of any changes)
— comments from involved parties, with initials and date
— results from re-tests.

The technology developer is responsible for documentation of changes to software necessary to solve an agreed finding. Software version numbers of the simulator(s) used during testing should also be documented.

#### 4.3.5.5 Site acceptance test

After installation of the product on board the vessel, the product will be subject to integration testing and network testing towards other systems and components.

Integration testing:

A test interface used to exchange signals between the target control systems, components and/or the simulator, should be defined and documented by the maker of the control system. This could be based on the normal I/O interface or a dedicated HIL interface. The interfaces will be subject to approval by DNV GL.

The scope of integration testing should be according to [4.3.5.2] and [4.3.5.3].

Network testing:

Network testing should be performed to evaluate the performance and integrity of the communication system, to detect any failures and enable preventative maintenance of networked equipment.

Test report from the site acceptance test of the system:

This document will include all observations from the FAT and site acceptance test, including the results of any re-testing. The test report from the site acceptance test should be updated throughout the project with:

— grading (including history of any changes)
— comments from involved parties, with initials and date
— results from re-tests.

The technology developer is responsible for documentation of software changes necessary to solve agreed findings from the FAT. Software version numbers of the simulator(s) used should also be documented.

#### 4.3.5.6 Updates and testing during operation

DNV GL shall be notified of any changes to the target system, including software and documentation, in accordance with DNVGL-RU-SHIP Pt.4 Ch.9 Sec.1 [1.5]. The notification should contain the reason for change and the impact on the target system and the operational philosophy. (for description of the change management process for software during operations, see [2.8.3].

All changes should be pre-tested in a safe test environment (e.g HIL/SIL test setup) and have the possibility of rollback to previous version. Access control and authority of change should be strictly controlled to avoid any unauthorized software changes.

Systems which include machine-learning mechanisms should be trained with defined datasets before the systems are deployed, and the system-capabilities in operation should be updated only at discrete intervals after successful verification and validation of the updates.

#### 4.3.5.7 Documentation

— software test reports; to be sent to DNV GL for information
— simulator test reports; to be sent to DNV GL for information
— simulator models; to be sent to DNV GL for information
— system test reports; to be sent to DNV GL for information
— change notifications; to be sent o DNV GL for information.

# SECTION 4 NAVIGATION FUNCTIONS

## 1 Introduction

### 1.1 General

This subsection provides guidance to the design and arrangements of systems supporting autonomous and remote operation of vessels, with the objective to ensure a level of safety of navigation that is equivalent or better compared to a conventional vessel where navigation is performed by navigators on board. Further guidance to arrangements in the remote control centre is given in Sec.6.

Guidance is also given to systems providing decision support to conventional manned vessels.

App.C provides considerations on the carriage requirements for navigational systems in SOLAS V/19, 19-1 and 20 for autoremote vessels.

App.D provides guidance on additional navigational systems for autoremote vessels.

The design of the primary navigational functions is regulated by applicable IMO conventions. Applicable conventions in this respect are the International Convention for Safety of Life At Sea - SOLAS, the International Convention for Preventing Collisions at Sea - COLREG and the International Convention on Standards of Training, Certification and Watch-keeping for Seafarers - STCW, as amended.

The above regulations are based on navigators on board having a full situational awareness based on own perceptions and situation analysis, supported by the aids prescribed by the regulations. The guidance to each of the different topics in this section is divided in two parts. The first part (Baseline) gives a description of the objective with the related regulations, and forms the functional requirements for which an equivalent safety level should be obtained. The second part (autoremote vessels) provides considerations on how these objectives can be met when the navigator's presence on board is replaced by autonomous and remote navigation.

The primary navigation related functions that should be covered during normal operation of the vessel will be addressed. These are general principles and the technical requirements are dependent on the various levels of autonomy and remote control.

### 1.2 Hazards

As previously explained as part of the process establishing the CONOPS in Sec.3 [2], a preliminary risk analysis (HAZID) should take place to evaluate the vessel's ability to operate safely and reliable. Hazards for the navigation function will depend on location and operational mode of the vessel, i.e. if during departure/ arrival or during transit. Based on such HAZIDs the following hazards are examples that are found to be typical to the navigational function:

— collision/contact with dock
— collision with other vessels
— collision/contact with pleasure crafts or persons in water
— collision/contact with foreign objects/obstacles (non-detected and detected)
— unexpected manoeuvres and drive-off
— collision with other vessels or pleasure crafts when sailing in reduced visibility
— grounding due to loss of propulsion
— grounding due to loss of steering control
— grounding due to deviation from planned route
— grounding due to error in planned route
— unable to follow COLREG due to errors in propulsion and steering
— loss of communication with remote control centre
— cyber security breaches
— sabotage, e.g. blocking vessel fairway

— other vessel calling to agree on a non-COLREG compliant meeting situation
— hitting fishing equipment/nets in fairway
— instability due to shifting cargo etc.
— unable to detect sound signals from other vessels or people
— unable to detect vibrations and heavy movements in the vessel
— unable to detect degradation of navigational sensors
— inability to detect deterioration of own performance
— too much trust/confidence in vessel autonomous action in critical situations
— failure in mooring sequence.

## 1.3 Degree of autonomy and division of function control

Based on the operational requirements and hazards to the navigation set forward as part of the CONOPS/ HAZID, one may define the navigational functions or tasks intended to be covered by autonomous systems and which to be covered by a human operator. In addition, the location of the human operator may be defined; i.e. if on board or remote. This should end up in an autoremote infrastructure that in total will give a level of safety equal to or better than a traditional vessel. As there may be varying abilities for systems to comply with an autonomous functionality that will cover all navigational functions, a mix of human and system operated tasks is assumed.

**Table 1 Levels of autonomy for navigation functions**

| *Autonomy level* | *Description of autonomy level* |
|---|---|
| M | Manually operated function. |
| DS | System decision supported function. |
| DSE | System decision supported function with conditional system execution capabilities (human in the loop, required acknowledgement by human before execution). |
| SC | Self controlled function (the system will execute the operation, but the human is able to override the action. Sometimes referred to as 'human on the loop'. |
| A | Autonomous function (the system will execute the function, normally without the possibility for a human to intervene on the functional level). |

As explained above, a function may be covered by a varying degree of autonomy; hence it is necessary to break the degree of autonomy further down. Below is a method that may be used to clarify which part of a function that is intended to be solved by a human and which to be solved by a system.

Initially the control of a function can be divided into four main parts:

— Detection:
Acquisition of information that is relevant for control of a function. The information may be based on sensors and/or human perceptions.
— Analysis:
Interpretation of the acquired information into a situational understanding relevant for control of the function.
— Planning:
Determination of needed changes in control parameters in order to keep the function performance within the applicable frames.
— Action:
Effectuating the planned changes of control parameters, typically via actuators operated via a control system. This is however considered to be conventional systems based on existing technologies, accordingly this guideline does not provide any further guidance for this.

Dividing the control of a function into the above elements is in general suitable for any function, but is in particular relevant for the navigation function as illustrated in Figure 1.

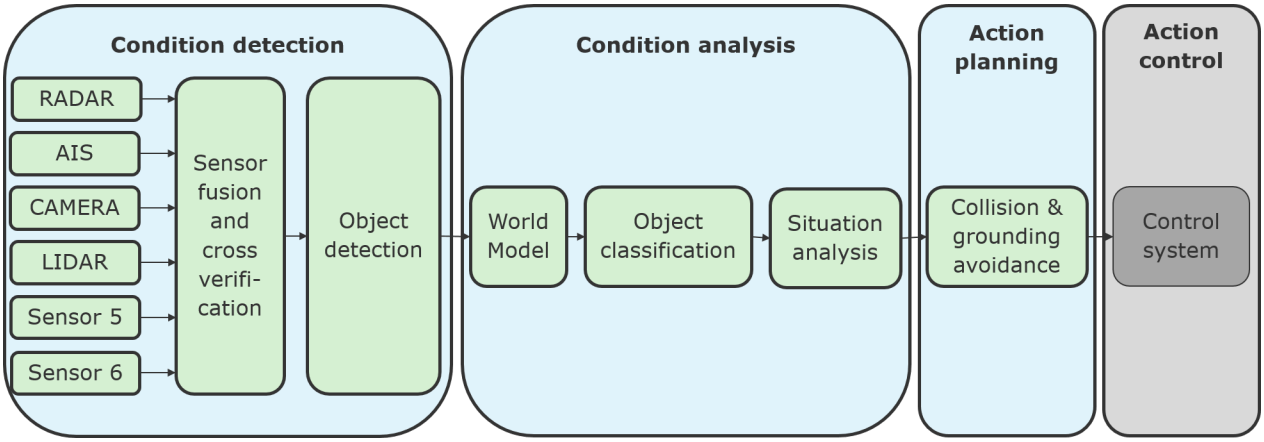


**Figure 1 Control of a function**

Each of the elements can be performed by either a human or machine (system), or the combination of the two. This is illustrated in Figure 2.

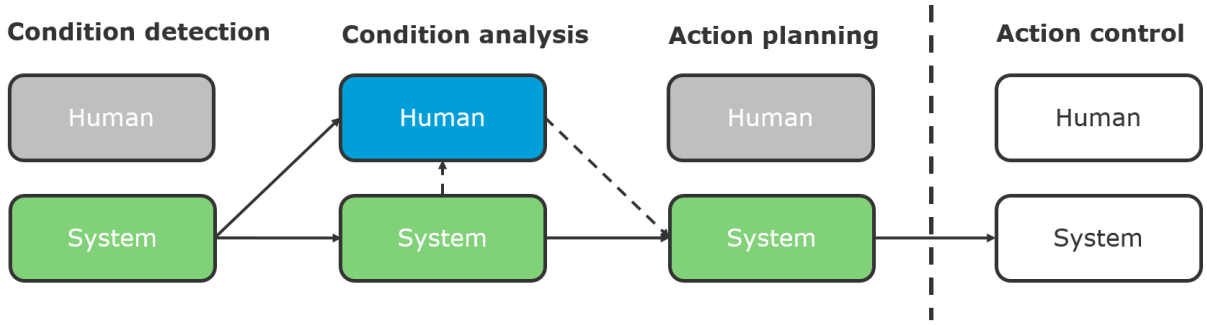


**Figure 2 Control of a function - manual or system**

The main principle is that the combined human/machine capabilities for one element (e.g. condition detection) should be the same or better than the conventional capabilities. This in order to achieve an equivalent or better level of safety.

Considering the example in Figure 2 where the lookout and collision avoidance functions are partly performed by a computer system instead of a human:

— Condition detection:
The vessel is fitted with an object detection system having capabilities that are equivalent to or better than that of a human (look-out) on board.
— Condition analysis:
The system has limited object recognition capabilities and depends on a human (e.g. in the remote control centre or by an OOW on board) to recognise and classify objects. The human would in this case need sufficient information about the object to ensure a correct object classification.
— Action planning:

Based on the object classification information, the system has capabilities to calculate an updated passage plan in accordance with COLREG that are equivalent or better than that of a navigator on board the vessel.

— Action control:
Based on the updated passage plan, the system or an OOW on board/remote may execute the updated plan.

The applicable navigation functions as described below and the technical guidance to the remote-control centre as described in Sec.6 are building on these elements of control when providing guidance to the technical design of automatic navigation systems and remote control centres. These elements of control are also supporting the modular approach with technology qualifications described in Sec.3 [1].

# 2 Planning prior to each voyage

## 2.1 Baseline

It shall be possible to plan the intended voyage in advance, taking into consideration all pertinent information and make a passage plan. Prior to commencing all the needs shall be determined, taking into consideration any requirements for fuel, water, lubricants, chemicals, supplies and any other requirements.

From a navigational perspective, it shall be possible to plan the voyage using adequate and appropriate charts and other nautical publications necessary for the intended voyage, containing accurate, complete and up-to-date information regarding those navigational limitations and hazards which are of a permanent or predictable nature and which are relevant to the safe navigation of the vessel. Before commencing the voyage the voyage plan shall be validated with regard to general grounding avoidance criteria and with regard to ability to follow the intended voyage plan based on environmental conditions and expected traffic conditions.

## 2.2 Autoremote vessels

The planning may be performed manually by personnel in the remote control centre (RCC) with the aid of support systems. The planning may also be done automatically by a system. If verification of the voyage plan is required, the system would fall under the category of a decision support system with conditional execution capabilities (DSE). The remote navigator should then acknowledge the plan before departure, having a scope as described in [2.1].

The remote workstation for navigation should as a minimum be provided with identical aids as the workstation for navigation planning on a conventional vessel. The need for any additional arrangements to compensate for that the planning is done in a remote location should be considered as part of the concept process described in Sec.3 [2].

# 3 Condition detection

## 3.1 Baseline

### 3.1.1 Proper lookout

Facilities supporting the principles in COLREG rule 5 of maintaining a proper lookout and the subsequent design criteria from SOLAS V/22 shall be a part of the vessel design. These facilities shall serve the purpose of:

— Maintaining a continuous state of vigilance by sight and hearing, as well as detection of significant change in the operating environment.
— Fully appraising the situation and the risk of collision, grounding and other dangers to navigation.
— Detecting ships or aircraft in distress, shipwrecked persons, wrecks, debris and other hazards to safe navigation.

#### 3.1.1.1 Horizontal field of vison

Facilities supporting a horizontal field of vision (FOV) to the horizon of 360° around the vessel shall be provided.

#### 3.1.1.2 Vertical field of vision

The view of the sea surface forward of the bow to 10° on either side shall not be obscured by more than two vessel lengths or 500 m, whichever is less, under all conditions of draught, trim and deck cargo.

The view of the sea surface from 10° on either side of the bow to 112,5° on either side shall not be obscured by more than 500 m.

The view of the sea surface from 112,5° to straight aft on either side shall not be obscured by more than 1 nautical mile.

#### 3.1.1.3 Blind sectors

Blind sectors caused by obstructions appearing within the forward 225° sector shall be as few and as small as possible. No blind sector caused by cargo, cargo gear or other obstructions which obstructs the view of the sea surface as seen from the main navigation reference location shall exceed 10°. The total arc of blind sectors shall not exceed 20° in the forward 180° sector and shall not exceed 30° in the forward 225 degree sector. The clear sector between two blind sectors shall be at least 5°. Over an arc from right ahead to at least 10° on each side, each individual blind sector shall not exceed 5°.

#### 3.1.1.4 Pitching and rolling

It shall be possible to detect all external objects of interest for safe navigation, such as ships, buoys and lighthouses in any direction when the vessel is pitching and rolling. In this context the horizontal and vertical field of view shall be sufficient to enable the equipment to fulfil the above performance requirements as well as being able to see the horizon.

#### 3.1.1.5 Field of vision for docking

As part of the docking operations situational awareness of the area surrounding the vessel shall be provided. In this context, the following view/awareness shall be supported:

— view/awareness of the sides of the vessel down to the water line
— view/awareness of area between vessel's water line and pier
— view/awareness of area close to stern and bow
— view/awareness of pier
— view/awareness of mooring gear location and condition.

#### 3.1.1.6 Lights, shapes and signals

It shall be possible to detect and recognise lights and shapes as described in COLREG Part C, and sound and light signals as described in COLREG Part D.

### 3.1.2 Determination of own position for grounding avoidance

The vessel shall be equipped with navigational and position keeping equipment necessary to execute a safe voyage plan. In this process, there shall be a possibility to determine the vessel position by use of various and independent positioning methods or a combination of such. As a general rule, position determination shall be based on minimum two independent methods.

#### 3.1.2.1 Applicable methods for determination of vessel position

1) Relative terrestrial by use of optical methods/sensors. With reference to performance requirements for bearing devices:
   — Optical sensors used for taking bearings shall have the capability to take bearings of distant objects whose altitudes are between 5° below and 30° above the horizontal.
   — Horizontal maximum relative bearing error shall not exceed 0.3°.
2) Relative terrestrial by use of electronic, non-optical means

— radar range/bearing
— range finder
— soundings
— radio fixing aids
— sonar ranges

Of the above it is assumed that the radar range and bearings are the most common used today.

3) Dead reckoning.
Upon loss of continuous positioning or between position fixes a method or system for determining the position based on vessel movement between other position fixes.

4) Electronic Position Fixing System (EPFS) suitable for the waters to be navigated.

#### 3.1.2.2 Operational requirements for position fixing

Operational requirements for position fixing shall comply with the minimum requirements set out in IMO Res. A915(22), A1046(27) and MSC.1/Circ.1575. Based on this the absolute position accuracy with 95% probability shall be:

1) For navigation in ocean waters - 100 m.
2) For automatic collision avoidance operations and navigation in harbour entrances, harbour approaches and coastal waters – 10 m.
3) For manoeuvring in port – 1 m.
4) For automatic docking operations - 0.1 m.

#### 3.1.2.3 Operational requirements for accuracy of electronic navigational charts (ENC)

The accuracy of nautical charts is defined by zones of confidence (ZOC). The ZOC required for safe operation will depend on how the navigation function is carried out and the operation area.

Based on this the ENC quality should be:

1) For navigation in ocean waters - ZOC C or better.
2) For automatic collision avoidance operations and navigation in harbour entrances, harbour approaches and coastal waters - ZOC A1 or better.
3) For manoeuvring in port - ZOC A1 or better.
4) For automatic docking operations - ZOC A1 or better.

## 3.2 Autoremote vessels

The conventional condition detection for the navigation function is obtained by a combination of conventional navigation equipment and human sight and hearing (look-out). The human contributions to condition detection will have to be compensated for when this task is performed by remote personnel in combination with systems. e.g. may an autoremote vessel need 2 electronic position fixing systems (EPFS) based on different underlaying technologies.

### 3.2.1 Condition detection by human

Direct substitutes for the sight and hearing are image and audio transmissions to the RCC, see Figure 3.

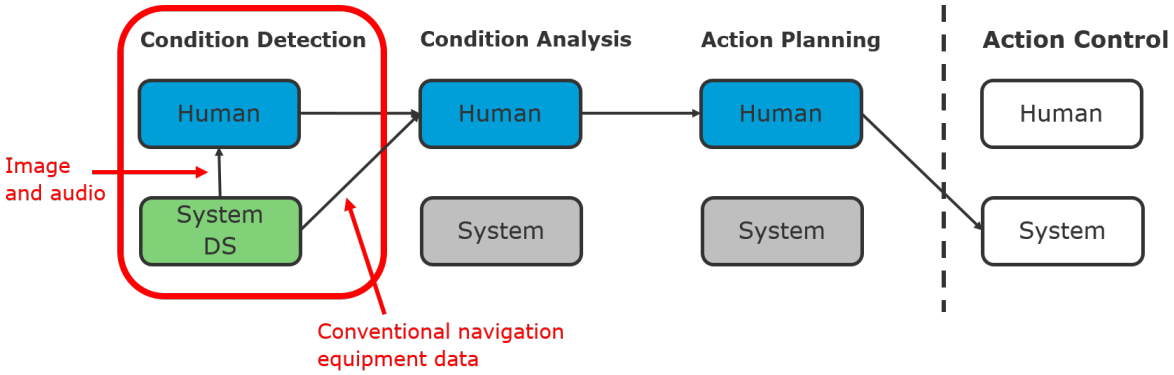


**Figure 3 Control of a function - Image and audio**

In order to obtain an equivalent capability for the remote operator to detect objects, the image transmission would need to be continuous with resolution, frame-rate, color depth and field of view providing an equivalent level of detection capability compared to a manned bridge. This is believed to be a challenging solution for a whole voyage, considering latency and the capacity limitations in communication links. It may however be relevant for parts of a voyage, e.g. for docking operations.

If a concept is based on condition detection in form of image and audio transmissions to the RCC, the condition detection function should be subject to risk analysis for all the operations it is intended to cover, taking into consideration limitations such as latency, capacity and reliability of the transmission, and factors that may affect the situational awareness when observing an image compared to real sight.

### 3.2.2 Condition detection by system

Continuous transmission of high definition images covering a wide sector may not be a feasible solution during all operational phases. Object detection by humans based on image and audio transmissions will also make a further condition analysis and action planning by systems challenging. In order to enable remote navigation watch for parts or the whole voyage, it is considered a necessity that the vessel is provided with an object detection system. An object detection system with verified performance capabilities providing an equivalent safety level will then replace the need for situational awareness with respect to object detection in the remote workstation for navigation, see Figure 4.

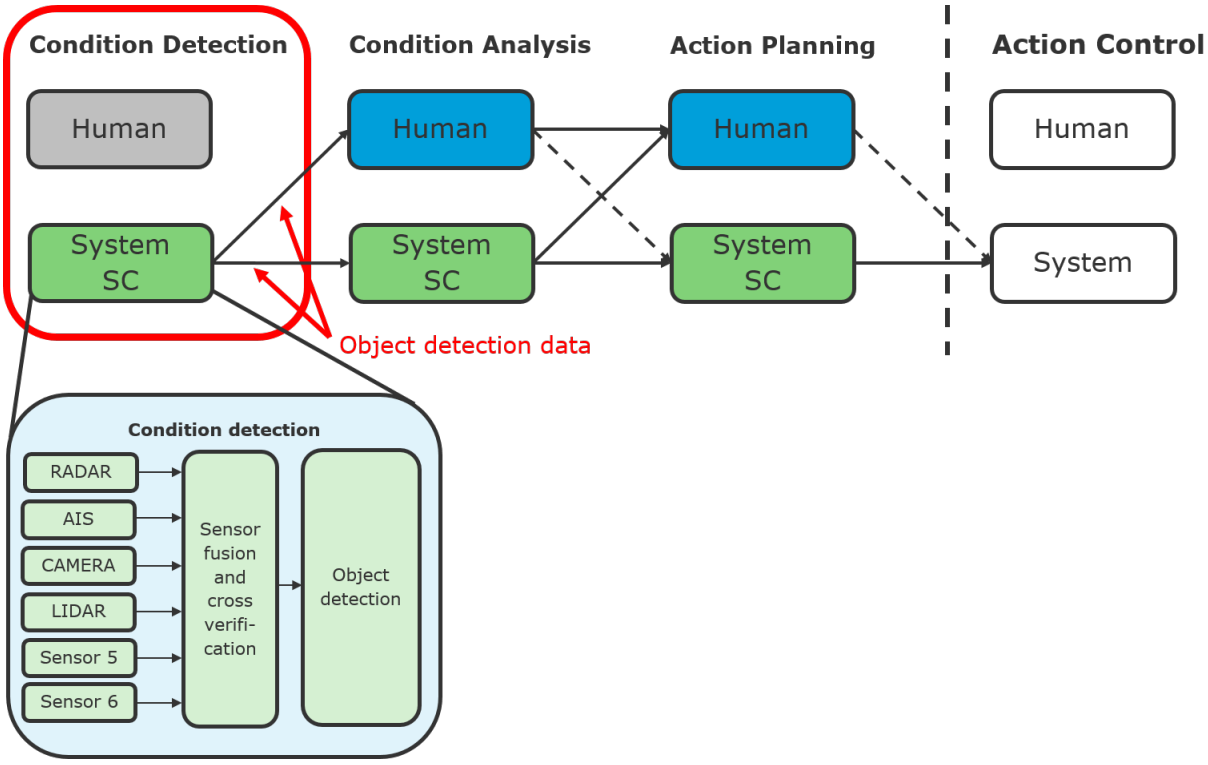


**Figure 4 Condition detection (look-out) by system**

### 3.2.3 Performance parameters for object detection systems

When an object detection system is intended to be used in a concept to replace the look-out function on board, the needed performance of the system to obtain an equivalent or better object detection capability should be determined as part of the concept process described in Sec.3 [2].

Any systems provided for detection of hazards to navigation above the water surface should be able to provide essential information supporting collision avoidance and safe navigation based on the requirements for lookout and horizontal and vertical field of vision described in [3.1.1]. Typical hazards include other vessels, aids to navigation, small unlit boats, floating logs, oil drums, containers, buoys, ice, hazardous waves, etc., thus the size, colour and material of the object are parameters to be considered.

Additionally, in clear weather conditions, other ships should be possible to be visually detected at any time in accordance with the visibility specifications for navigational lights - see COLREG Rule 22. Other hazards should be possible to detect at a distance that allows the vessel to make evasive maneuvers in order to avoid the object in question.

The specific detection-range requirements should be decided per concept qualification project and will depend on ship-type, size, maneuverability and speed.

# 4 Condition analysis

## 4.1 Baseline

Facilities supporting the classification of objects detected should be provided.

Classification of other vessels should include the ability to distinguish between the following vessel classes - see COLREG Rule 18:

— power-driven vessels underway
— vessel not under command
— vessel restricted in her ability to manoeuvre
— vessel engaged in fishing
— sailing vessel.

In addition to the above, facilities supporting the classification of objects that are hazardous to the navigation but not covered by COLREG should be provided. Consequently, objects located in the water that are not hazardous to the navigation should also be classified as non-hazardous. Examples of hazardous objects may by containers, large logs, small boats (canoe, kayak etc.), ice, and buoys. Non-hazardous objects typically are seabirds.

## 4.2 Autoremote vessels

A sufficient situational awareness necessary to analyse a navigational situation should be obtained by the personnel responsible for remote navigation in the RCC. The situational understanding should ensure that the navigation can be planned and executed with an equivalent or better safety compared with the situational understanding obtained by navigators on board.

In order to plan (or alternatively supervise) that navigation is performed in a safe way following COLREG, it will not be sufficient for the remote navigator only to know whether or not surrounding hazards have been detected. The remote navigator will also need to analyse the complete navigational situation, i.e. consider the hazards in relation to other factors that may affect the further navigation planning, such as location, movements and type of a hazard, other potential hazards in the surroundings, the risk of grounding, the weather conditions and sea states, and the own vessel's operational mode and capabilities.

Conventional vessels with navigators on board are fitted with sensors and systems aiding the navigator in obtaining a situational awareness for analysing the navigational situation, such as radars, ECDIS, AIS and instruments showing own vessel's condition. The complete situational awareness is obtained by merging the information provided by these aids with information the navigator obtains from own senses, such as sight, hearing and vessel movements. When navigation is performed from a remote location, the sensor data should be presented to the remote navigator in such a way that the objective to obtain an equivalent situational understanding is achieved.

### 4.2.1 Image transmission

The purpose of a visual presentation of the surroundings in the context of situation analysis is not to enable detection of hazards, but to visually present sensor information to the remote navigator ensuring an equivalent situational understanding for condition analysis.

For this purpose, the image presentation may not necessarily be continuous and with high definition. The image should however be sufficient for the remote navigator to perceive all relevant surrounding conditions that will have influence on the situation analysis.

When the human sight is substituted by image transmissions, it should be taken into consideration that most images are two-dimensional, which means that depth and distances are difficult to estimate. This may be necessary to compensate for depending on the navigational situation. If a three-dimensional image is not possible to achieve, this should be compensated for, e.g. by additional distance sensors and merging a graphical presentation of this into the image presentation.

### 4.2.2 Virtual models

Use of different sensor technologies, the fusion of the sensor data and representation in a virtual model may provide an equivalent situational awareness for a remote navigator compared to transmitted images.

When such virtual presentations are used, it should be ensured that all relevant human perceptions are reflected, including vessel movements such as roll and heel, and understanding of ambient conditions. A suitable and sufficient virtual presentation should be considered in the concept process, taking into consideration relevant factors resulting from the operational area of the vessel and the vessel features.

### 4.2.3 Object classification

The human or system responsible for planning the navigation needs to receive a classification of the detected objects in order to plan the navigation in accordance with COLREG.

#### 4.2.3.1 Object classification by human

If object recognition is based on human analysis as illustrated in below figure, the remote navigator will need to receive an image of the object. The image of the actual object should be with sufficient high definition to enable the remote navigator to classify the object, see Figure 5.

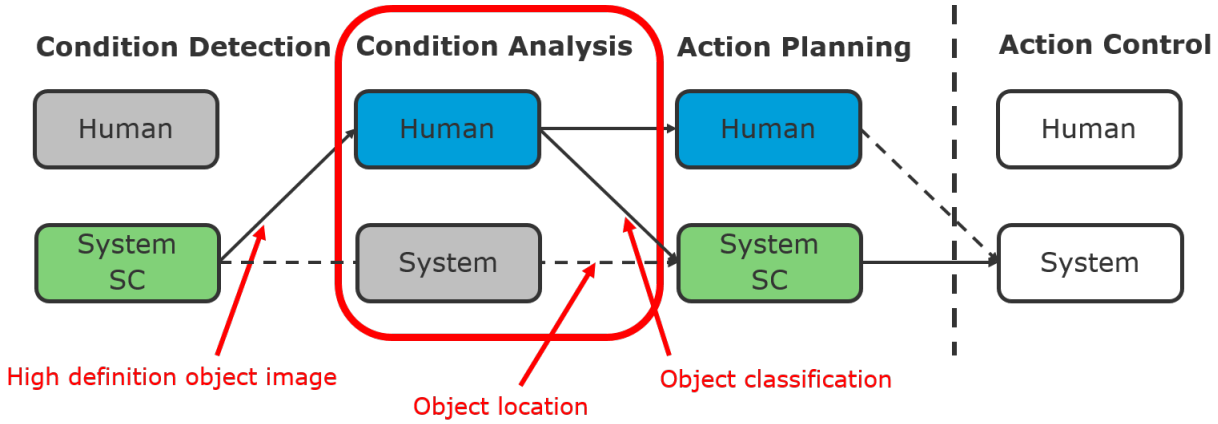


**Figure 5 Object classification - manual**

Needed resolutions of images will depend on different factors such as types of hazards relevant for the operational area, the type and size of objects that may impose a hazard for a specific vessel, and the speed and the manoeuvring capabilities of the vessel and accordingly from which distance an object needs to be classified. When object classification for a concept is based on human analysis, the needed image resolution should be considered in the concept process described in Sec.3 [2].

#### 4.2.3.2 Object classification supported by AIS

Technology may be used to support in the classification of objects, see Figure 6. An example of such technology is the AIS, which may provide digital information sufficient to classify other vessels for the purpose of navigation in accordance with COLREG.

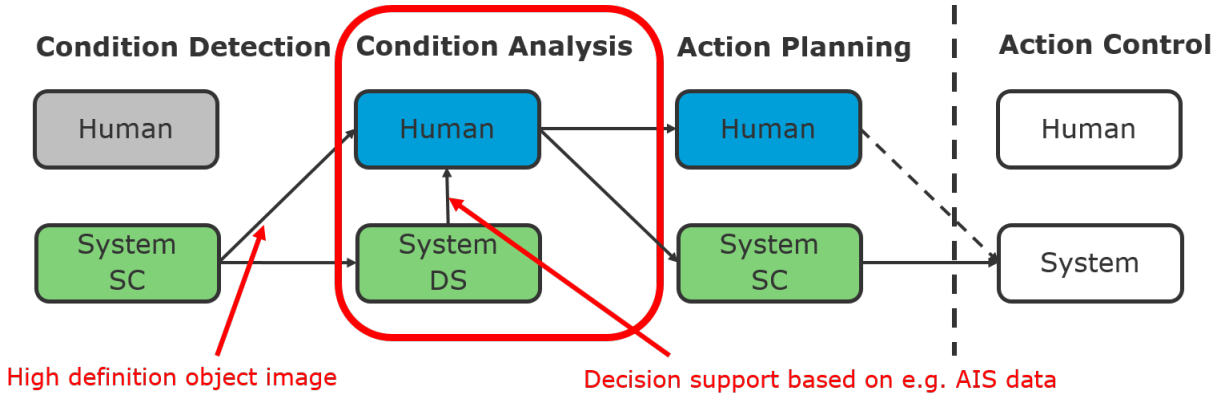


**Figure 6 Object classification - decision support**

The AIS will only aid in object classification of other ships that are equipped with AIS. Vessels not equipped with AIS and other objects identified as hazards by the object detection system will have to be classified by other means. Further, the AIS information from the other vessels is to some extent based on manual data input. The correctness of the AIS information (e.g. whether a fishing vessel is trawling or sailing) may be uncertain. It is thus considered that object classification based on AIS information should be in form of decision support, i.e. to be acknowledged by the remote navigator based on independent observations. The independent observation may be e.g. in form of image transmission as described above. See also Sec.6 [5.2] regarding independent supervision.

#### 4.2.3.3 Object classification supported by recognition technology

Object recognition is a technology under development. The state of the technology for marine applications are presently at a research level. Subject to a technology qualification as described in Sec.3 [4], it may be considered in a concept process whether a technology has sufficient capabilities to provide an independent verification for classification of certain objects. The decision support system may then have conditional execution capabilities (DSE), i.e. system decided object classification without human acknowledgement for certain objects as illustrated in the figure below. This would require the system to ask the navigator for assistance to classify an object in case confirmed classification is not possible to achieve by AIS data and object recognition, see Figure 7.

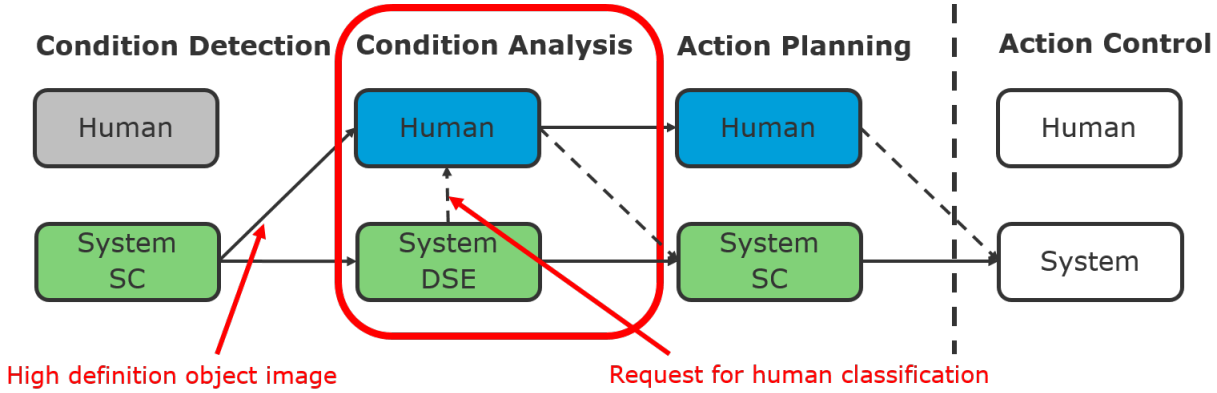


**Figure 7 Object recognition - DSE**

# 5 Deviation from planned route

## 5.1 Baseline

If required during the voyage to deviate substantially from the planned route, then an amended route shall be possible to be planned and validated before execution of the deviation.

Facilities supporting the principles of COLREG rule 7 and 8 in determining the risk of collision and actions to avoid collision shall be part of the vessel design.

If determined that there is a risk of collision and actions are taken to avoid collision, there shall be facilities supporting the rules of COLREG Section II - *Conduct of vessels in sight of one another* and Section III - *Conduct of vessels in restricted visibility*.

## 5.2 Autoremote vessels

### 5.2.1 Workstation for voyage planning

A workstation for voyage planning should be provided in the RCC to enable navigators to carry out passage planning and chart works while taking in nautical publications without interfering with ongoing remote navigation of the vessel. The workstation should be equipped with means for efficient voyage planning and means for direct transfer of the planned voyage to other navigating workstations as relevant.

The need for a separate workstation for navigation planning should be considered as part of the concept process, taking into consideration intended personnel with intended tasks and responsibilities, the level of autonomy and trading route (e.g. trade in regional waters having adequate coverage of ENCs). See also Sec.6 [1.2.2] regarding manning in the RCC.

### 5.2.2 Manual route planning

If the deviation from the planned route is done by the remote personnel as illustrated in Figure 8, the performance of this function from the RCC will correspond to the conventional performance of the function with a navigator on board.

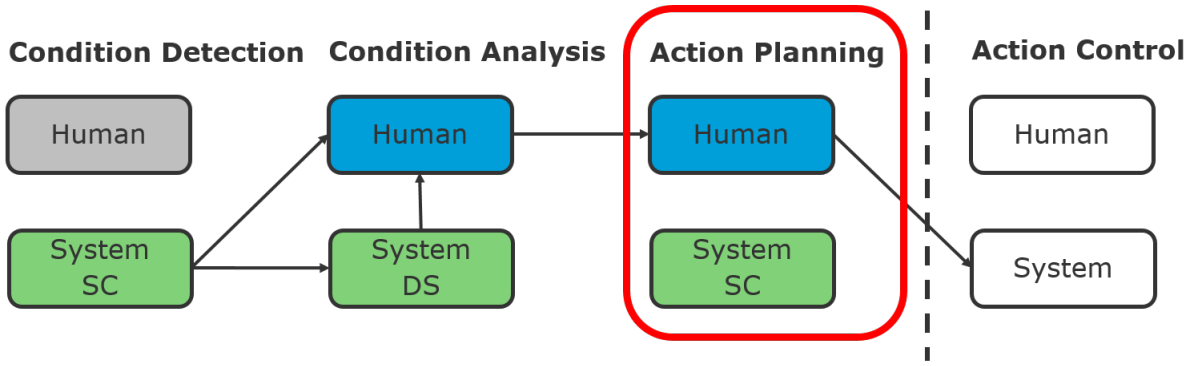


**Figure 8 Manual route planning**

Based on observed hazards or other changes in the conditions affecting the planned route, the navigator will analyse the situation and change the orders to the autopilot, either by updating the route plan or direct change of orders. A remote navigator should have obtained an equivalent situational awareness compared to an on-board navigator with respect to condition detection and analysis. This should provide a sufficient basis for the remote navigator to plan and execute a new route. It should be part of the risk analysis in the concept process to consider whether additional arrangements will be needed for planning and executing the navigation in the remote workstation beyond what is described in [4.2] for situational awareness.

### 5.2.3 Decision supported route planning with condition based execution

Planning and execution of collision avoidance may also be done by a system. Depending on verified performance capabilities as part of the technology qualification of the system (see. Sec.3 [4]), the planned action control may require verification (acknowledgement) by the remote navigator before execution (DSE). The system may also have limitations with respect to the navigation complexity it is capable of handling, and may ask the remote navigator to plan the actions. An illustration of this is given in Figure 9.

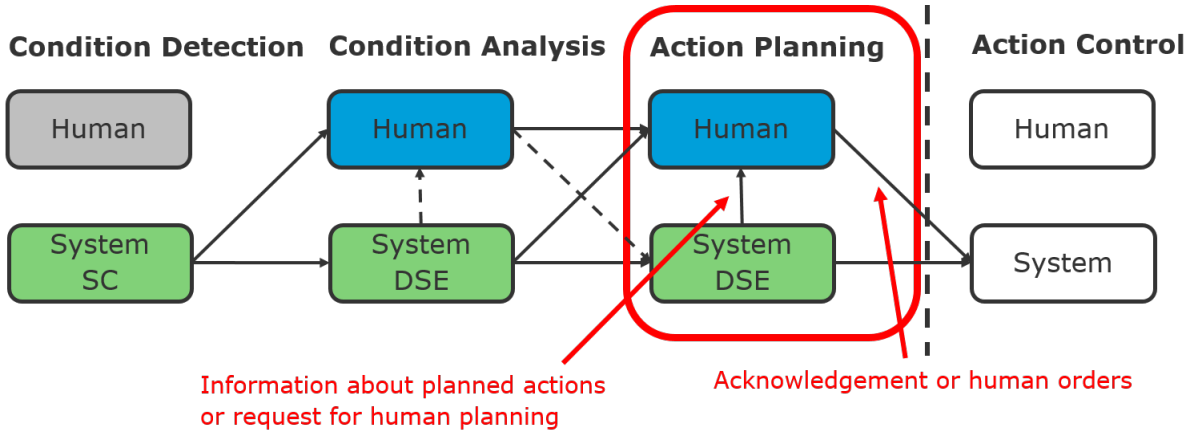


**Figure 9 Collision avoidance - DSE**

If the concept for a project is based on handing over the action planning to the remote navigator for complex situations, the remote navigator should have the same situational awareness as for the manual route planning. If the concept for a project is based only on acknowledgement of intended actions, the remote navigator should be provided with independent information for supervision as described below in [5.2.4] for self-controlling systems. It should be part of the concept process to evaluate capabilities of the technology and to ensure a sufficient situational awareness for the remote navigator according to the tasks.

### 5.2.4 Self-controlled route planning

If collision avoidance is planned and executed by a self-controlling (SC) collision and grounding avoidance system, the remote navigator will have a supervising role as illustrated in Figure 10.

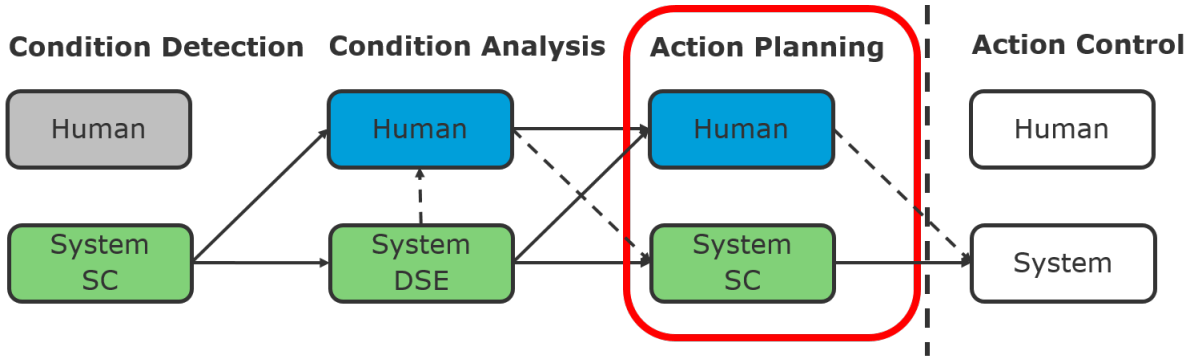


**Figure 10 RCC - self-controlled route planning**

The vessel should automatically be brought to an MRC in case the navigation situation exceeds the complexity the system is designed to handle. It is not expected that action planning should be handed over to the remote navigator for self-controlling systems. The remote navigator should however have the possibility to intervene and initiate an MRC as a minimum.

The remote navigator should be provided with information sufficient to do independent analysis of the conditions and make independent conclusions on what the appropriate control actions should be. Further, the collision avoidance system should clearly indicate, together with a pre-warning, the updated plan before the intended control orders are executed, leaving the remote navigator with sufficient time to do own observations and analysis, and intervene if required.

It should be part of the concept process to consider the system's capabilities to handle complex situations, the intended tasks by the remote navigator in case the complexity is exceeded, and the related need for situational awareness and independent supervision for the remote navigator.

### 5.2.5 Performance criteria for collision and grounding avoidance

Parameters necessary to support the baseline guidance for collision and grounding avoidance is driven by the abilities for object detection and classification and the abilities to determine the risk of collision and action to avoid collision. In addition, the following parameters are deemed important to systems intended to comply with the navigational role:

— complexity of the hazards to navigation, like the number of objects to relate to
— transparency of planned movements
— solidity of algorithms used in COLREG compliant systems.

# 6 Contingency plans

## 6.1 Baseline

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

## 6.2 Autoremote vessels

The requirement in [6.1] forms the baseline for the MRCs.

Applicable emergency events should among others include loss of communication between RCC and the vessel. For vessels under the responsibility of remote operation from the RCC, automation systems on board the vessel should have capabilities to autonomously bring the vessel to an MRC without the need for directions or supervision from the RCC. This should be initiated based on the system's own detection of loss of communication with RCC, as illustrated in Figure 11. This includes detection of loss of passive supervision by RCC.

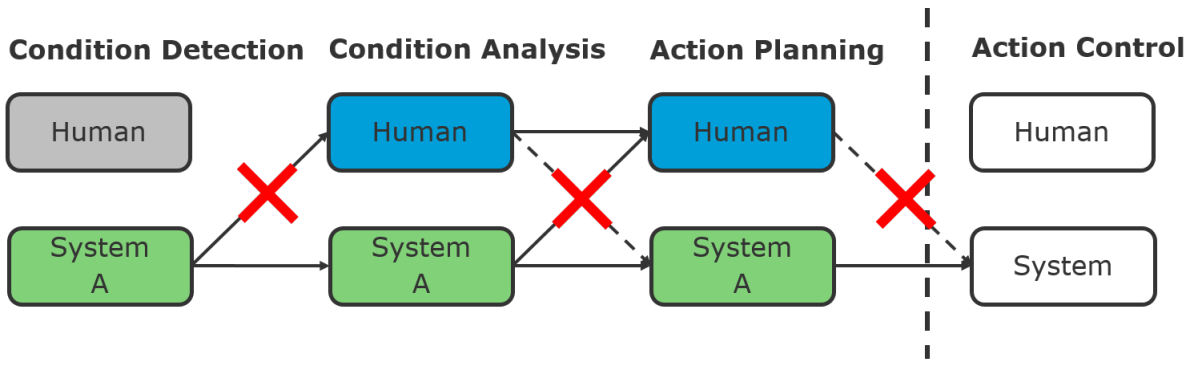


**Figure 11 RCC - Autonomous MRC**

The autonomous system for planning and executing the autonomous control of a vessel to an MRC should be supported by systems having autonomous condition detection and condition analysing capabilities providing sufficient situational awareness for the task to bring the vessel to an MRC.

Also the personnel in the RCC responsible for the operation should have the possibility to decide on entering an MRC in case of other emergency events. The autonomous system on board should accordingly also be capable to autonomously bring the vessel to an MRC based on input from the RCC.

Relevant MRCs will depend on the operational area and the capabilities of the vessel. Different MRCs may be planned for different legs of a voyage. The operational complexity of MRCs may range from dropping the anchor to continuing the voyage. A list with examples of potential MRCs are given in App.A. It should be taken into consideration that MRCs based on a high degree of operational complexity will result in the need for an autonomous system capable of handling a corresponding high degree of complexity, as well as having advanced self-monitoring capabilities.

This guideline does not include any considerations with respect to whether a vessel should be capable of following statutory regulations in case of operations during an MRC. It should be in the scope of the concept submitter and the relevant administration to respectively propose and approve acceptable MRCs for the area of operation, including acceptable restrictions in the vessel's manoeuvring capabilities and suitable signals to indicate this.

MRCs covering the whole voyage should be planned and implemented in the vessel's autonomous system prior to departure. See also Sec.6 [5], providing further guidance to remote control and supervision related to MRCs.

# 7 Safe speed

## 7.1 Baseline

Facilities supporting the principles of COLREG rule 6 of the vessel at all times to proceed at a safe speed shall be part of the vessel design. In this context, this implies a situational awareness based on factors like:

— traffic situation
— weather- and sea conditions
— area of navigation with regard to manoeuvring characteristics of the vessel and hazards along the intended route or track.

In general, safe speed implies that the vessel based on these factors at any time shall be able to either stop or deviate from the intended voyage plan in time to avoid collision with another ship or to avoid a hazard.

## 7.2 Autoremote vessels

Vessel speed may be planned and executed either by the remote navigator or by a system. When the vessel speed is planned and executed by the remote navigator, the remote workstation should be arranged with information with respect to the relevant factors ensuring a situational awareness equivalent to the awareness for a navigator on board. If safe speed is planned and executed by a system, the remote navigator should be provided with sufficient information for supervision. It should be part of the concept process to consider relevant information needed and the need for independent supervision.

# 8 Manoeuvring

## 8.1 Baseline

The vessel shall be equipped with facilities for safe ship manoeuvring and handling. In addition to the facilities supporting proper lookout, the following shall be supported when manoeuvring the vessel:

— Proper visual near vessel information.
— Effects of deadweight, draught, trim, speed and under-keel clearance on turning circles and stopping distances.

— -Monitor the ship's heading, rudder angle, propeller revolutions, propeller pitch (if relevant) and thruster(s) (if relevant).
— The effects of wind and current on the vessel.
— Effect two-way communication with other parts of the vessel organisation when required.

## 8.2 Autoremote vessels

For autoremote manoeuvring the need in the RCC for the situational awareness covering the baseline factors above will be influenced by the amount of autonomy which is built into the total autoremote infrastructure. Equipment used may be a combination of sensors like CCTV, radar and laser based systems and other detection technology that either give true images or electronic reproduction of the surrounding area in real or near real time. As previously mentioned the information flow may be challenging for the communication link when a large amount of data may be required to be transferred from the vessel to the RCC; hence high definition CCTV may be challenging and hence other systems suitable to get good situational awareness without the need for high data flow may be required.

# 9 Docking

## 9.1 Baseline

Facilities supporting safe docking of the vessel shall be part of the vessel design. For situational awareness of the field of vision requirements for docking operations and the facilities supporting safe manoeuvring as mentioned above shall be covered. In addition, the following tasks shall be supported:

— supervision of docking operations
— monitor the vessels's heading, rudder angle, propeller revolutions, propeller pitch (if relevant) and thruster(s) (if relevant)
— release of sound signals
— monitor the relevant mooring operations by having orders effected
— effect two-way communication with mooring stations on board and ashore
— effect two-way communication with other parts of the vessel organisation when required.

## 9.2 Autoremote vessels

For autoremote docking the above baseline requirements in general should support the situational awareness needed. The autoremote control may vary from more manual to automatic to autonomous operation. In this context, it should be noted that there today already exist systems of auto-docking that are not covering parts of specific IMO performance standards. In general, these are dynamic steering control systems that are intended to manage an automatic docking of the vessel; however without the ability of supervision and control related to external dynamic dangers to the operation. The need for situational awareness of the surrounding area of the vessel may require even more information than for the manoeuvring operations. Where the CONOPS establish fixed docking facilities, the supervision of the area of operation may well be enhanced by using local land based infrastructure with high bandwidth communication links to the RCC. This may reduce the risk of latency and heighten the redundancy of the required information.

# 10 Alert management for navigational functions

## 10.1 Baseline

To ensure good handling, distribution and presentation of alerts in main systems for navigation and required sub-systems/sensors, all navigation related alerts shall be managed in accordance with the BAM concept

of IMO as defined in MSC.302(87); hence by including a central alert management system - CAM. Other equipment shall be connected to the CAM if this is under the responsibility of the navigation function.

## 10.2 Autoremote vessels

A corresponding central alert management system should be arranged in the workstation for navigation functions in the RCC. See also Sec.6 [5.4].

# SECTION 5 VESSEL ENGINEERING FUNCTIONS

## 1 Introduction

### 1.1 General

This section provides technical design guidance for systems supporting remotely operated main functions as defined in DNVGL-RU-SHIP Pt.1 Ch.1 Sec.1 Table 2. This corresponds to the functions under the responsibility of the officer in charge of the engineering watch as defined in the STCW code.

The common guidance in [2] describes overall intentions and design principles governing the level of safety in accordance with DNV GL main class rules and how these principles should be considered for autonomous or remotely controlled vessel functions to obtain a safety level equal to- or better than that of a conventional vessel with functions controlled by on-board crew.

Incidents and failures in [3] provides guidance for component types, failure modes and incidents to be considered in the design of systems and components (i.e. abnormal conditions which should be considered in the risk assessment and give rise to redundant design).

The other subsections provide technical guidance for design of specific engineering functions.

Each subsection is introduced by relevant baseline requirements in SOLAS and/or DNV GL main class rules. The subsequent paragraphs provide technical design guidance deemed necessary for autoremote vessels to achieve a level of safety equivalent to the baseline.

### 1.2 Extent of automation and support from personnel on board

Remotely controlled vessels without personnel on board can only achieve an equivalent or increased level of availability and safety if the tasks currently carried out on board are either eliminated (i.e. automated) or performed by operators in a remote control centre (RCC).

In addition, important vessel functions should generally be arranged with fault tolerance or redundancy to compensate for failures and incidents which cannot be handled by manual work on board.

The design guidance in this section assumes that the vessel is operated with remote engineering watch as defined in Sec.1 [3]. Any design alleviation due to assistance by personnel on board is given where applicable. Document *Concept of Operation* should specify which, if any, tasks can be performed by personnel on board, see Sec.3.

Furthermore, this design guidance assumes that remotely controlled vessel functions will require a certain level of automation to aid the operator in RCC. This guidance defines two main categories of automation, see below.

The objective is to differentiate between tasks needing active involvement by personnel versus tasks which will be automatically performed by automation system(s).

— automatic support (AS)

  Operation of the vessel function by automation systems and personnel in combination. Automation system(s) may partly or fully perform data acquisition, interpretation and decision. This mode is a collective term for all variants of decision support where the automatic support function may need complementary human sensing, interpretation or decision-making and where the action is not automatically effectuated.

— automatic operation (AO)

  Operation of the vessel function by automation system(s) without need for intervention by personnel. Unwanted and unexpected events and situations (outside operational design domain) are automatically handled by on-board safety system(s) to ensure the ship will remain in a safe state (within the last resort MRCs). Personnel will supervise the operation and may intervene.

Document *concept of operation* should specify the relevant automation mode for every operational task. Ship functions and systems needed to perform the operation should be arranged with capabilities supporting the respective automation mode.

# 2 Common guidance

## 2.1 General

In general, the principles listed below reflect design criteria to ensure minimum level of availability and safety for traditionally manned vessels in DNV GL main class rules (baseline). A brief comparison with autonomous and remotely operated vessels is given for each principle.

## 2.2 Redundancy and function restoration

The following provides general guidance related to redundancy and restoration of key vessel functions listed in Sec.2 [6] sorting under the engineering role.

### 2.2.1 Baseline

Vessel main functions as defined by DNVGL-RU-SHIP Pt.1 Ch.1 Sec.1 Table 2 should be arranged with redundancy type 2. This implies that crew on board shall be capable of restoring operation of a main function within 10 minutes.

The essential functions propulsion and steering shall be arranged with redundancy type 1 (max 30 sec. to re-establish function).

See DNVGL-RU-SHIP Pt.1 Ch.1 Sec.1 Table 2 for further details and/or exemptions to the above baseline principles.

### 2.2.2 Autoremote functions

Since autonomous or remote controlled vessels will be operated with reduced or no manning on board and since such vessels may have different safe states (MRC) than conventional ships, the extent and type of redundancy may vary depending on the intended operations of the vessel.

Consequently, the terminology main functions and essential functions are not applied for autonomous or remote controlled vessels - instead the term key functions denote vessel functions which are deemed to be important for autoremote vessels.

### 2.2.3 Redundancy and automation

Level of redundancy, fault tolerance and extent of automation for the systems supporting any key function in Sec.2 [6] should be the result of the conceptual design process described in Sec.3. I.e. document concept of operations should describe each operational mode and its corresponding MRC.

Corresponding risk assessment(s) should analyse the effect of failures and incidents and conclude on system design concepts in support of the overall design principles in Sec.2 [9].

Depending on the outcome of the risk assessments and the defined MRCs , any temporary loss of vessel functions may not be acceptable.

### 2.2.4 Restoration of functions

It should in general be possible to restore a key vessel function from the RCC without assistance by personnel on board. Depending on the failure or incident causing stop of the function, the restored function may have reduced capacity.

Restoration of the function should be assisted by a decision support system (AS) or performed by an automation system (AO). See also local/manual actions below.

For vessels with personnel on board, local/manual restoration by on-board crew may be relied upon if adequate competence, instructions or assistance by RCC is available.

## 2.3 Local/manual actions

The following provides general guidance on how local/manual tasks performed by operators on conventional vessels should be considered for autoremote vessels.

### 2.3.1 Baseline

For conventional vessels, it is accepted that local/manual action is needed to re-establish a vessel function. This implies that on-board crew must be able to perform local control of machinery and other equipment, including minor repair-work and replacement of components.

### 2.3.2 Autoremote vessels

For autoremote vessels, it is generally not considered feasible to mitigate effects of failures and incidents by manual actions performed on board. Even for ships with a limited crew on board, the crew may not be expected to perform in-depth troubleshooting, repair or replace faulty components, employ manual fire guards, restore backup systems, etc.

For this reason, additional compensating measures should be implemented to cope with failures and incidents to achieve a safety level equivalent or better compared to conventional vessels.

Key vessel functions should be arranged with sufficient redundancy and automation to eliminate or reduce the need for local operations, repairs and other physical work during operation. This may imply independent means of control from RCC if deemed necessary by relevant risk assessment(s).

Means should be arranged on board to compensate for failure in the remote control system in RCC and in related communication equipment and controls. Such compensating means should be able to control the vessel or its equipment to a safe state (within MRC).

Personnel on board should only be given responsibility for assisting tasks in the following conditions:

— When the tasks have been defined as part of the vessel design (e.g. CONOPS).
— When personnel on board have sufficient competence/skill.
— When the amount of planned work on-board is manageable for the personnel on-board.
— When clear procedures have be established.
— When communication with operators in the RCC is available allowing instructions to be provided.
— When decision support systems are available for the personnel on board as needed.
— When an unambiguous human/machine interface is provided in a centralized control room.

### 2.3.3 Automatic Operation (AO)

Even if conventional manual operations on board will be replaced by purely automation systems, capabilities for remote supervision and emergency control should be arranged in the RCC.

The automation systems should be located on board and not be affected by failures in communication links or external systems.

Additionally, to compensate for alternative manual ways to cope with unexpected and abnormal events on conventional ships, such automation functions should be redundant or augmented by independent automatic safety systems.

As an example, a power management system on a conventional vessel is in general not provided with redundant control. Upon failure of the automatic control, the state of the electrical power system will remain unchanged and manual control by qualified crew on board will be possible. To compensate for manual control, the power management function should be redundant for vessels where the power system is designed for automatic operation.

If additional automatic control functions are implemented in systems remote to the ship, failures to such systems should be handled by automation/safety systems or personnel on board.

### 2.3.4 Automatic Support (AS)

If conventional manual operation on board will be performed by the remote engineering watch in RCC, decision support functions should be arranged which provide a firm basis for making decisions and executing control actions.

# 3 Incidents and failures

## 3.1 General

As described in Sec.3, risk assessments should be done as part of the conceptual design and during detailed design. The primary objective is to ensure that risks associated with expected and abnormal variations, failures and incidents are mitigated by designing necessary redundancy or fault tolerance into the vessel and/or its connected systems.

The incidents and failures in [3.2] to [3.11] should be considered examples of possible "events" indicated in the MRC-illustration in Sec.2 [5]. The list is not exhaustive, hence additional failure modes should be included as deemed necessary to meet the design principles in Sec.2 [9].

Failures should in general be detected and initiate automatic actions resulting in the least critical of any possible new condition (i.e. fail-to-safe principle). Recording and alarming should follow the principles in Sec.6 [5.8]. Fail-over to backup systems should in general be automatically performed and require no manual interaction.

### 3.1.1 Baseline

Active components such as pumps, fans, electric motors, generators. (see DNVGL-RU-SHIP Pt.4 Ch.1 Sec.1 Table 1). Failure of such active components shall not cause loss of the functions served and the components must be arranged with redundant design or by alternative ways to remain operational, e.g. by manual intervention by the crew on board. Certain components, such as main engine, shaft, gear and propeller, are exempted from the redundancy requirement (see DNVGL-RU-SHIP Pt.4 Ch.1 Sec.3 [2.3.5]).

Failure of passive or static components such as pipes, valves etc. is in general not considered within main class in this respect. This approach is partly based on the lower probability of failure in static components and partly on the assumption that required detection/alarm/protection systems are implemented so that personnel on board may respond to such abnormal events and avoid propagation.

Incidents of fire and flooding with subsequent loss of a space is generally not considered as design criteria for machinery arrangements within main class. The main class approach is - similarly as for static components - i.a. based on the assumption that fire outbreaks are detected, automatically or by the crew, and that the fire-fighting systems on board and crew intervention may handle the situation.

### 3.1.2 Autoremote vessels

For autoremote vessels, due to the limited presence -or absence of crew to perform manual intervention, any failure modes and incidents that would depend on manual intervention on conventional ships should be included in the risk assessments and be appropriately compensated for by means of redundancy, fault tolerance and automatic functionality in the design.

Failures of components defined as active in DNVGL-RU-SHIP Pt.4 Ch.1 should also be considered for autoremote vessels, and furthermore, the types of failures to be considered should be extended as described in [3.1.3].

The main class exception of considering failures in certain active components (e.g. main engine, shaft) is generally not applicable for autoremote vessels unless justified by compensating measures such as e.g. the presence of responsible personnel on board, enhanced predictive diagnostic functions, condition based maintenance programmes.

### 3.1.3 Failure categories

To meet the design principles in Sec.2 [9], failures and incidents to be analysed in the risk assessments are generally divided into two categories:

1) anticipated failures

   Anticipated failures are failures that are expected to occur in the future. Such failures may typically be due to wear and tear, clogging, process variations or similar. Unconventional arrangements and systems and components having limited records of reliable operation for the application should also be considered subject to an anticipated failure.

The effect of such failures should be mitigated by redundant design and should not cause the function being served to stop working. The vessel should be able to continue operation and its planned voyage, possibly at reduced speed/capabilities. However, the fault-tolerance of the systems affected by the failure may in such cases be reduced, which may in turn necessitate mitigating actions or even operational limitations - depending on the operational mode. Specifications for this should be established in the concept process described in Sec.3 [2].

Each paragraph in [3.2] to [3.11] includes guidance if the failure modes are considered anticipated.

2) potential failures

Potential failures are failures that are less probable than anticipated failures, but may still occur sometime during the vessel's operational life. Upon such failure, the vessel should be able to enter and maintain a safe state / MRC. Failures in this category that may impair functions needed to maintain this capability should be included in the risk assessments and potentially lead to redundant design and segregated arrangements. Such failures may then cause a temporary stop of the function being served, but should not prevent restoration by the redundant system. At least the failure modes listed in [3.2] to [3.11] should be considered.

### 3.1.4 Redundancy

When redundancy of vessel functions and/or systems has been designed as a result of the prescribed risk assessments, the following principles apply.

Functions and systems designed with redundancy should be able to maintain or restore its function when one failure has occurred. Redundancy can be achieved for instance by installation of mutually independent components or by mutually independent systems capable of performing the same function. Redundancy type should in general be R0, i.e. continuous availability, unless justified otherwise. See DNVGL-RU-SHIP Pt.4 Ch.1.

Mutual independence means that the function of the redundant components or systems, their power supply and other auxiliaries, should not depend on any common component or system. See DNVGL-RU-SHIP Pt.4 Ch.1.

Each redundant system should be subject to risk analysis as part of the concept processes described in Sec.3, with the objective to identify and mitigate common-cause failure modes. The failure analysis should at least include failure modes in [3.2] to [3.11]. If single fault tolerance cannot be demonstrated through such failure analysis, additional mitigating measures, e.g. segregation, should be included in the design.

### 3.1.5 Failure response and detection

The following provides general guidance related to the effects of a single failure.

#### 3.1.5.1 Baseline

Failures shall be detected, alarmed and lead to a safe state. Safe operation of conventional vessels is largely based on:

- Detection of a single failure. If a single failure is not detected, any subsequent failure should be considered.
- Effect of a failure leads to safe state, considering the equipment under control and the vessel in general.
- Many failures and incidents can be responded to by the crew on board, i.e. by restoring the failed service or initiating compensating countermeasures.

#### 3.1.5.2 Autoremote vessels

The above principles apply also for autonomous and remotely controlled vessels. However, increased redundancy, more automation, improved HMI/alert management and a more rigid definition of safe state should be part of the design to compensate for reduced capabilities for local/manual intervention.

The types of failure modes to consider should be extended and systems should be designed with more sophisticated diagnostic functions (e.g. condition/health monitoring) to detect evolving failure conditions and hidden failures.

Additionally, subsequent effects of a failure on related functions or connected systems should be considered in the risk assessment and compensated by fail-to-safe behaviour, prioritization schemes or automatic activation of reversionary controls/safety functions.

## 3.2 Fire

Any compartment or space containing equipment or systems that impose a risk of fire should be addressed in the risk assessment. The propagation and extent of a fire casualty is determined by several factors, such as presence of combustible material, fire detection/extinguishing capabilities and the fire rating of bulkheads and decks surrounding the origin of the fire. Consequently, these factors determine the fire casualty threshold, i.e. the possible locations of fire origin as well as the probable extent of fire casualties. In the event of such fire casualties, the systems that must remain functioning to enable the vessel to enter and maintain an MRC should be arranged with appropriate redundancy, segregation and/or protection to ensure continued functioning.

For autoremote vessels in a trade/operational pattern where the defined MRCs demand continued operation of the key vessel functions, the risk of fire should normally lead to duplicated and segregated arrangement of systems serving such key functions.

The concepts, definitions and interpretations of fire risk, casualty threshold, fire survivability of SOLAS Ch.II-2 Reg.21 *Casualty threshold*, safe return to port and safe areas may be used as a basis, taking into consideration differences such as increased probabilities due to limited or lack of crew, and reduced consequences due to the absence of passengers.

In the context of this guidance, failures caused by fire are not considered as anticipated failure modes.

## 3.3 Flooding

The risk of flooding following an internal leak, e.g. flange rupture, should be considered for any watertight compartment exposed to piping systems or other possible sources of leakage. The extent of a flooding would normally be limited by the boundaries of the watertight compartment, and any equipment within that casualty threshold should be considered lost unless adequately protected, e.g. by an IP rating corresponding to the maximum water column.

Similar to the fire scenario, any equipment or systems needed for the vessel to enter and maintain the defined MRCs should therefore be arranged with appropriate redundancy and segregation, or IP protection.

In the context of this guidance, failures caused by flooding are not considered as anticipated failure modes.

## 3.4 Failures in rotating machinery

Failure of rotating machinery, such as engines, shafts, gear, generators, electrical motors, pumps, fans should be considered in the risk assessments.

Failures of rotating machines are in general considered as anticipated failures. Redundancy should be arranged to ensure continued normal operation of the vessel, i.e. be able to continue the planned voyage. The capacity of the function after a failure may be reduced compared to maximum capacity, but the function should perform within the specifications for normal operation (see [3.1.3]).

Failure of rotating machines may be considered as potential failures, and not anticipated failures, if confidence can be obtained that the component is healthy, i.e. not in the process of deterioration and not subject to impending break-down. Such confidence should be provided by advanced and well proven diagnostic functions, and may be considered for type of machines subject to failures propagating over time. Relevant diagnostics information should be logged and stored (see Sec.6 [5.8]).

## 3.5 Failures in other mechanical components

Failure of other mechanical components such as valves, filters, heat exchanges. should be considered in the risk assessments.

The probability of failure will vary between the different types of components. Whether such components should be considered subject to anticipated or potential failure, or possibly exempted as a failure mode, should be considered in the risk assessment.

## 3.6 Electrical failures

Electrical failures should be considered in the risk assessments for all systems, including power generation, power distribution and associated control systems.

As a minimum, following failure modes should be considered as anticipated failures:

— short-circuits and earth faults in electrical equipment, including cables
— failure of a power generating equipment
— failure of a power converter
— failures of a UPS
— failure of power generation control (e.g. governor and AVR)
— failure of power/energy management systems
— transient under-voltages in the system caused by short-circuits
— failures causing partial black-out.

As aminimum following failure modes should be considered as potential failures:

— failures causing complete black-out
— fire and flooding within a casualty threshold.

## 3.7 Failure of control systems and safety systems

Failure of electronic components and software should be considered in the risk assessment(s) for all units supporting vessel key functions. Systems with increased reliability and/or safety integrity, or other similar improvements, are not acceptable in lieu of redundancy.

Software-related errors should be considered as relevant (e.g. lacking functionality, communication errors, HMI errors, errors in handling of faults, coding errors/bugs such as bad logic or data type mismatch).

For redundant components serving critical vessel functions, common mode software failures should be considered. Compensating measures may include using software from different manufacturers covering the same function such that both will not fail simultaneously due to a SW error.

Failures related to integration of different control systems (incompatibility, protocol differences, exception handling, etc.) and failures related to transition between operational modes (e.g. delayed or missing signals) should also be addressed in risk assessments where relevant.

Safe states should be defined and demonstrated, including continued operation in degraded mode and fail-over to redundant systems. In consideration of fire and flooding, multiple failures are considered relevant and should be evaluated (e.g. loss of redundancy link with subsequent loss of main controller).

Wire break, loose connection, sporadic failure of hardware components and communication errors should be considered anticipated failures.

## 3.8 Failure of data communication networks/links

Logical failures caused by, for example, wrong configuration, inadequate design, component defects, wrong connections should be considered in the risk assessments.

Conventional failure modes such as loss of power to network switches, wire break and connection faults should be considered anticipated failures.

See also Sec.7.

## 3.9 Cyber security incidents

Incidents related to cyber systems should be considered in the risk assessments.

Such incidents are not considered anticipated failures provided adequate precautions are implemented, see Sec.7 [4.5].

## 3.10 Human errors

Human error should be considered in the risk assessments. Examples may be inadvertent operations due to ambiguous HMI, wrong connection of network cables and signal wires, unawareness, misinterpretation of conditions and scenarios, poor judgement due to stress, colour blindness, sickness/injuries, etc.

Such incidents are not considered anticipated failures.

## 3.11 External events

Events occurring external to the ship should be considered in the risk assessment. Such events could be foreseeable but unexpected, or foreseeable and predictable. These could lead to operational challenges depending on human response, capability of automation systems or robustness of systems/components. Examples are severe weather conditions, unexpected objects in the vicinity of the ship and other events requiring high performance of the machinery.

Such events are not considered anticipated failures.

# 4 Propulsion and steering

## 4.1 Baseline

SOLAS Ch.II-1, Part C.

Means shall be provided whereby normal operation of the propulsion machinery can be sustained or restored even though one of the essential auxiliaries becomes inoperative. Special consideration should be given to the malfunction of systems and components subject to anticipated failure. (Interpretation of SOLAS Ch.II-1 Reg. 26.3).

Systems and components supporting the propulsion function shall be arranged with redundancy and capacity sufficient to ensure that the vessel can maintain a navigable speed in case of potential failures of single systems and components. (Interpretation of SOLAS Ch.II-1 Reg. 26.2).

DNVGL-RU-SHIP Pt.4 (main class).

The propulsion and steering systems including necessary auxiliary systems shall provide the capability to control and maintain minimum safe speed and vessel direction in all expected operational modes, including expected external variations such as severe weather conditions. This includes the capability to maintain or restore sufficient propulsion/steering capacity within 30 seconds in the event of failure of certain defined active components.

## 4.2 Autoremote vessels

To fulfil the above intentions for autoremote vessels, additional arrangements compared to conventional ships may be needed to compensate for less or no personnel on board. Such arrangements may be increased separation, increased redundancy/fault-tolerance, adequate/reliable remote operator interface and autonomous functions ensuring safe response to failures.

The terms propulsion system and steering system should be understood to include necessary auxiliary systems such as fuel, cooling, power, control systems.

If thrust is needed in any direction to enter and remain in an MRC, the propulsion or steering function in this context will also include thrusters and the systems supporting these.

### 4.2.1 Redundancy and capacity

The propulsion and steering systems should be arranged with capacity and redundancy sufficient to ensure continued normal operation in case of anticipated failures. The vessel should be capable of continuing the voyage as planned without any substantial loss of any propulsion/steering capacity. Criteria for normal operation with respect to propulsion capacity and speed of the vessel should be subject to specifications as part of the concept process.

If any part of a contingency plan for a voyage (see Sec.4 [6]) has a last resort MRC that depends on propulsion, the propulsion system should be arranged with capacity, redundancy and separation sufficient to ensure that the vessel can enter and maintain the last resort MRC under all potential failure conditions. This should take into consideration events such as fire or flooding. A casualty threshold for fire and flooding should be established as part of a concept process (see [3.2]), defining the containment boundaries for fire and flooding casualties.

As described in [3.1.2], the failure of a propulsion engine should be considered as a failure mode for vessel operations without any assisting personnel on board. Such vessels should accordingly be arranged with minimum two independent propulsion lines.

For vessel operations with assisting personnel on board, the need for redundancy in propulsion lines should take into consideration the capabilities of the on board personnel to mitigate effects of failures and incidents by manual actions. See also [2.3]. Such considerations should be subject to risk analysis in the concept process.

A vessel arrangement with two propulsion lines is in general considered to meet the objective of continued normal operation in case of loss of a propulsion line. The propulsion should then be arranged with capacity sufficient to meet the specifications for normal operation after loss of any one propulsion line.

### 4.2.2 Remote link/interface

The infrastructure providing remote control/supervision should be redundant/single fault tolerant.

Autonomous system(s) should be arranged on board to ensure that safe state (within MRC) is maintained in the event of problems with the remote interface.

If responsible personnel are available on board, problems with remote communication/systems should issue an alarm on board. The objective is to supervise the automatic operation, establish communication with RCC and to manually initiate emergency procedures / other local controls as relevant.

### 4.2.3 Main command locations

#### 4.2.3.1 Vessel speed and direction

The main command location for control of vessel speed and direction should be at the location of the responsible navigating officer (if the navigation function is remotely controlled, the responsible navigator will be in RCC, otherwise the responsible navigator will be on vessel bridge).

This implies that if personnel are available on board, it should not be possible to take control privilege for control of vessel speed and direction unless permission is granted by the responsible navigator.

The same applies for the engineering watch in RCC - control of vessel speed and direction should not be possible unless permission is granted by the responsible navigator.

#### 4.2.3.2 Propulsion and steering machinery

The main command location for control of propulsion and steering machinery should be at the location of the responsible engineering watch in RCC.

If personnel are available on board, it should not be possible to take control privilege of control of propulsion/ steering machinery unless permission is granted by the engineering watch in RCC. Such controls should have restricted access and be designed in accordance with the competence and availability of on-board personnel.

Engine telegraph should normally not be required.

#### 4.2.4 Safe state

Safe mode of a propulsion or steering system and its supporting auxiliary systems should normally be fail-to-maintain.

#### 4.2.5 Automatic support (AS)

If the propulsion or steering function is arranged with decision support functionality, following applies:

- All manual actions taken by the engineering watch in the control of propulsion and steering machinery including handling of abnormal events should be aided by a decision support system.
- The decision support system should issue a warning in case the operator chooses actions which may lead to undesirable events.
- The decision support system should be integrated with other systems (e.g. navigation, power system.) to ensure that the operator does not choose actions which may cause hazards or undesirable effects in the other systems.

#### 4.2.6 Automatic operation (AO)

If the propulsion or steering function is arranged to be automatically operated (AO):

The automation system should fully control propulsion/steering machinery and supporting auxiliary systems in all defined operational modes. The engineering watch in RCC will supervise the operation and may intervene if deemed necessary.

The automation system may be arranged such that the responsible personnel is given a notification or warning in due time before it carries out an order. The operator may then choose abort or modify the order.

It should be possible to manually intervene and control the propulsion/steering system from the RCC.

No manual actions should be needed to maintain or restore the propulsion or steering function or to ensure the ship reverts to safe state if needed.

The engineering watch in RCC should be provided with sufficient monitoring, alerts, diagnostic functions and controls to intervene in case of unexpected events and failures which are not safely handled by the automatic control functions. This may be based on aggregate status information (e.g. green, yellow, red light) with the possibility to efficiently drill down for identification of abnormal or unexpected conditions. See also Sec.6 regarding remote vessel control and supervision in RCC.

# 5 Electrical power supply and distribution

## 5.1 Baseline

SOLAS Ch.II-1, Part D.

A main power supply system, including power generation and distribution, should be arranged with redundancy and capacity in such a way that electrical power supply sufficient to ensure normal operation of the vessel can be maintained or restored in the event of system or component failures, including the failure of any generating set. The main electrical power supply system should be self-contained, ensuring that power supply from the sources of power to the main switchboard may only be affected by a fire or other casualty within one casualty boundary. (Interpretation of SOLAS Ch.II-1 Reg. 41).

An emergency power supply system, including power generation and distribution, should be arranged with capacity sufficient to handle emergency conditions and maintain the vessel in a safe state. The emergency electrical power supply system should be self-contained, ensuring that the power supply from the emergency source of power to the emergency switchboard may only be affected by a fire or other casualty within one casualty boundary. The emergency power supply system should further be arranged in a location ensuring that emergency power supply can be maintained under any emergency condition. (Interpretation of SOLAS Ch.II-1 Reg. 42).

The main and emergency power supply systems should be mutually independent in such a way that power supply to functions essential for handling an emergency condition and maintaining the vessel in a safe state is ensured in case of fire and other casualties within any casualty boundary. (Interpretation of SOLAS Ch.II-1 Reg. 41 and 42).

## 5.2 Autoremote vessels

Power supply generation and distribution should be arranged with sufficient redundancy, capacity and automatic functions to ensure equivalence to baseline considering the vessel's intended autoremote functionality, level and responsibility of manning on board and failures outlined in [3]. This includes the capability to maintain normal operation and handle emergency conditions in the event of relevant abnormal situations.

### 5.2.1 Main power supply

A main power system should be arranged with redundancy and capacity sufficient to ensure normal operation in the event of an anticipated failure (see [3.1.3]).

Required vessel performance and corresponding power capacity to ensure normal vessel operation should be defined in the concept process described in Sec.3 [2]. It should also be defined acceptable time to restore normal operation in case of an anticipated failure.

The risk analysis should identify all relevant failure modes, consider the probabilities of the failures (see also guidance in [3.7]) and analyse the effects these may have on the above objectives. The analysis should take into consideration the reduction or lack of personnel on board to assist in mitigating the effects of a failure.

If main power supply is necessary to ensure that the vessel can enter and remain in an MRC (e.g. power necessary for propulsion), the effects of fire and flooding, as well as other potential failure modes, should be included in the risk assessments.

### 5.2.2 Emergency power supply

SOLAS and main class requirements for emergency power supply will apply for concepts with personnel on board.

The same objectives to ensure power supply to consumers necessary to handle an emergency condition and keep the vessel in a safe state will apply also for vessels without personnel on board. Equivalent capabilities to ensure the safety of the public, the assets and the environment are expected.

The emergency services listed in SOLAS Ch.II-1 Reg. 42.2 will in general be relevant also for vessels without personnel on board. Even emergency lighting may be necessary in order for the remote operators to obtain a sufficient situational awareness in an emergency situation, although the areas that needs to be illuminated may differ. In addition, other services necessary in order to handle an emergency condition and to bring and maintain the vessel in a safe condition will apply.

The risk analysis should identify all relevant events that may result in an emergency condition, and analyse the effects these may have on the power supply to consumers necessary to handle the events and to bring and keep the vessel in an MRC. The analysis should take into consideration the reduction or lack of personnel on board to assist in mitigating the consequences of an event.

The principle of redundancy in power supply to emergency functions should apply for autoremote vessels as it applies for conventional vessel. On conventional vessels this redundancy is ensured either by redundancy in services (e.g. lighting in a space provided by both normal and emergency lighting), or by redundant supplies to the emergency consumers from respectively the main and emergency source of power. The same principle of redundancy in power supply to functions necessary to handle an emergency condition and bring and keep the vessel in an MRC should apply to autoremote vessels.

An arrangement with an independent emergency source of power in addition to the main source in [5.2.1] is one possible arrangement. Another possible arrangement is two independent and separated main sources of power according to DNVGL-RU-SHIP Pt.4 Ch.8 Sec.2 [3.1.4]

### 5.2.3 Power management

Some operational concepts may have duplication of machinery with operational profiles where only one engine is online, The risk of black-out should be considered, and special attention paid to the reliability of power restoration, considering the limited or lack of personnel on board to assist in this. In particular, the possibility for failure on demand of stand-by systems should be considered (i.e. hidden failures in stand-by systems not revealed until the stand-by functionality is required). As a minimum, the systems should be subject to an initial test prior to each voyage as described in Sec.6 [5.5].

In order to ensure availability of main power supply during critical parts of a voyage, the power management system should have an operation mode where the power supply system is set up in a redundant mode ensuring that no anticipated failures will result in a black-out, including transient voltage dips in the system caused by short-circuits. This operation mode should accordingly be with open bus-tie unless voltage dip ride through capabilities of the system have been documented.

The following automatic power management functions should at least be arranged:

— load dependent start of additional generators
— blackout prevention such as load reduction, limitation, shedding, start blocking, etc.
— blackout recovery.

Failures in the power management system should follow the "fail-to-maintain" principle, i.e. no change in power generation or distribution.

Electrical protection functions should be implemented in the respective electrical components (not in the power management system) and at the lowest possible level. The objective is to ensure that electrical failures are isolated close to the point of failure and will not affect both redundant power systems, even in case of loss of power management.

# 6 Control, monitoring, alarm and safety systems

## 6.1 Baseline

Control systems should in general comply with baseline requirements in DNVGL-RU-SHIP Pt.4 Ch.9 (main class).

## 6.2 Autoremote vessels

Control systems should in general comply with baseline requirements stated above. Additional guidance due to remote control from RCC and limited manual operations on board are given in the following sub-sections.

## 6.3 Design principles

### 6.3.1 Components

Electronic components installed on board should be suitable for marine use and comply with environmental requirements stated in the baseline in [6.1] (i.e. type approved in accordance with DNVGL-CG-0339.)

Field instrumentation and actuators should be suitable for marine use and comply with environmental requirements stated in the above baseline reference.

Maintenance, calibration, upgrade and other manual work should be scheduled and not be needed during the vessel's voyage.

For any system intended to be repaired by personnel on board, spare parts and replacement procedures should be available. Compatibility between installed components and spare parts should be ensured.

### 6.3.2 Power supply

Ship-shore communication and control systems needed for the vessel to enter and maintain MRC should be powered by UPS supplied from both main and emergency power systems. Redundant consumers should be powered by independent supplies.

### 6.3.3 Single fault tolerance

Any single failure in control, safety or automation systems should not prevent the vessel from entering and maintaining safe state (MRC). Systems and components should be arranged with redundancy, separation and/or independency as needed to ensure this principle.

Single failures should be analysed. It should be documented and possible to demonstrate that safe state can be maintained or reached upon each failure mode.

An anticipated failure should not prevent normal operation.

See also [3].

## 6.4 Control and monitoring

### 6.4.1 Status and situational awareness

It should be possible to observe real-time operational status, readiness and capacity of the vessel function or system from RCC. See also Sec.6.

Where responsible personnel are present on board, systems providing control, monitoring and alert functions should be arranged in one centralised location.

The remote operator in the RCC should achieve a situational awareness sufficient to ensure that the remote operation is performed in a safe way equivalent to when the function being performed by crew on board.

The required level of situational awareness for a remote operator of the engineering functions should be considered in view of automatic support and automatic control functions implemented to handle normal and abnormal conditions.

The existing requirements for unattended machinery space operations should be observed. Additional considerations should be given to human senses that contribute to detection of abnormal conditions. Examples of such may be detection of vibrations and high temperatures. For example, compensating measures could be used as described below:

— installation of regular/infrared cameras, microphones or vibration sensors in relevant locations
— communication solutions enabling efficient ship-shore collaboration. E.g. video-solutions, augmented reality, smart helmets, pagers.

### 6.4.2 Alerts

Abnormal conditions and situations should generate alerts that in general are categorised and prioritized in accordance with the principles of MSC.302(87) *Performance Standards for Bridge Alert Management*.

Responsibility for alerts should as default be in RCC. If responsible personnel are present on board or in another control centre, the responsibility for responding to alerts should be clearly indicated on each relevant work station. If response to an alert must be taken by operator on board, the alert should always be issued on board and a corresponding warning or caution should be given in RCC.

Alerts in RCC should not require information which can only be observed on board. Common alarms should be avoided.

If an alert is not responded to by the operator in RCC, the vessel should be able to reach or maintain safe state.

Irrelevant alerts should be automatically suppressed or not implemented.

Alarm systems on board and alarm systems in RCC should support seamless integration using the same message format/protocol. Either location should indicate the same status of an alert and any operator not responsible to respond should see when the alert has been acknowledged.

An alert should include descriptive and unambiguous text and include guidance to the operator about any actions to be taken. Self-evident actions such as standby start or re-instatement of redundant system should be taken automatically.

The engineering watch should not be presented with alerts which do not contribute to situational awareness or do not require any response/action (i.e. nuisance alerts).

For a function which is automatically operated (AO) no human action should be needed to maintain operation of the function or vessel safe state. Hence, alerts requiring intervention by the engineering watch should not exist unless warranted by special circumstances such as unexpected emergency conditions. Nevertheless, alerts (e.g. of priority caution) should still be provided for the engineering watch if action can be taken to rectify/improve the condition, or if the alert contributes to improved situational awareness (e.g. by pre-warning of impending events).

Manual emergency operation from RCC should be possible, but not necessary to enter and maintain safe state. For this reason, relevant alarms or emergency alarms should also be given in RCC as basis for activating such emergency controls.

### 6.4.3 Manual response to single failures

It should be possible to respond to failures with manual actions by the operator in RCC (i.e. to reduce the consequences of a failure, restart of systems, reset of failures, etc.).

Manual actions should not be needed to maintain- or revert to safe state.

For vessels with personnel on board, it should be possible to perform local manual actions subject to instructions from RCC and adequate competence of the on-board personnel. In such case, the system should be designed for such manual actions, e.g. intuitive interface, clear instructions, means to avoid inadvertent operations, etc. Such manual actions should not be needed for the vessel's capability to enter and maintain safe state. However, such manual actions may be appropriate to restore redundancy or increase capacity.

### 6.4.4 Indication and control on board

It should not be possible to access local controls on board by unauthorized persons.

Any system which is designed with means to perform control from on-board locations should be arranged with adequate indication (e.g. necessary process status, feedback of control actions, alerts, etc.) In addition, for any important vessel function where the machinery is designed with means for local control, there should be means for voice communication with RCC.

Only one location (on board/RCC) should possess the privilege for control of a vessel function or an EUC at any time and means for transfer of control should be arranged. The two control locations may not have the same capabilities, but if justified by document concept of operation, it should be possible to override or perform emergency control on board the ship.

### 6.4.5 Logging

See Sec.6 [5.8].

## 6.5 Integration

### 6.5.1 Failure of integrated systems

The effect of failure of integrated control, monitoring, alarm and safety systems should be limited and manageable for the personnel.

This principle takes into consideration that even for current conventional vessels, complex integrated systems may be crucial for safe operation. The operators depend on these systems and may not be sufficiently manned or trained to manually monitor and control all the machinery/equipment in local positions in the event of total failure of the integrated system.

For this reason, failures in such systems should be limited, predictable and manageable for the responsible operator/crew. Analysis functions should be available to aid the operator in advance on the effects of an eventual failure.

This functionality should enable the crew in RCC to know in advance how the vessel will automatically respond to the failure.

For vessels with personnel on board, this functionality should enable the crew on board to efficiently cope with the failure by local/manual actions and/or repairs as relevant (see previous paragraph).

### 6.5.2 Network arrangements

Networks should in general be arranged with redundancy and separation. This applies specifically for:

— networks used to integrate components serving multiple vessel functions
— any network where functionality of a connected device depends on information transmitted by the network (i.e. where a connected device cannot perform its intended functions without information received via the network).

Single networks are accepted for systems serving only one vessel function and where fault tolerance is not required. Where a single vessel function is served by two separated control systems, each system may be arranged with single network.

Control system components for the following functions and systems should not be connected to the same network segment:

— bridge/navigation systems
— required communication systems
— machinery control and monitoring systems
— safety systems and other systems needed to revert to safe state in case of any failure
— control systems serving redundant vessel services
— cargo systems
— administrative and other systems not related to vessel key functions
— systems from different system suppliers.

A programmable unit should not depend on information from a different network segment.

A programmable unit needed to maintain or revert to safe state should not depend on information transmitted via network (dedicated IO network or serial links are acceptable).

### 6.5.3 Communication with RCC

The guidance regarding the communication between the ship systems and the remote control centre is detailed in Sec.7.

## 6.6 Protective safety functions

### 6.6.1 Background

The intention of a protective safety function is to take the machinery or equipment to a safe state (normally shut down) in the event of specific abnormal conditions to prevent hazard to personnel, property or the environment.

All elements needed to achieve the safe state is considered part of the protective safety function (e.g. sensor, CPU, power supply, data communication, actuator). See also common definitions of safety instrumented function (SIF).

An abnormal condition which on conventional ships is intended to be responded to by personnel on board by use of local manual actions should either be considered a protective safety function or redundancy should be implemented to eliminate the need for manual action.

### 6.6.2 General

A protective safety function may be manually or automatically activated, ref. requirements in baseline and relevant DNV GL application rules.

Means for manually activating protective safety functions should be arranged in central and convenient locations on board and in RCC as relevant. Means to prevent inadvertent operation should be implemented.

Ship functions designed for automatic operation (AO) should have automatically operated protective safety functions.

Means to manually override protective safety functions should be implemented in RCC as needed.

Safe state for each safety function should be defined. Failure of any element constituting the safety function should generally lead to the same safe state.

If protected equipment necessary to ensure safety of the vessel (i.e. within MRC) has been defined to have safe state shut down, the protected equipment should be arranged with redundancy.

### 6.6.3 Arrangement

Safety functions should generally be implemented by use of dedicated components, independent from other functions as follows:

- Safety functions should not be implemented in the same system/component as control, monitoring or alert functions.
- Safety functions for redundant units or processes should not be implemented in the same system/component.
- Safety functions serving different units or processes should not be implemented in the same system/component.

## 6.7 Software

See Sec.3 [4] for guidance related to software development life cycle (SDLC) activities.

Novel software should not be deployed on autoremote vessels unless developed in accordance with SDLC processes. Verification and validation activities should normally include testing with proven simulation methods and include all relevant operational modes/abnormal incidents.

Software-based devices in the field layer (e.g. sensors) and control layer (e.g. PLCs) of the control, monitoring, alert and safety systems should be dedicated to a particular vessel key function.

COTS software should generally not be used in the field layer or control layer of systems used for vessel key functions. Real-time operating systems intended for industrial applications should be used.

All software in a device should be identified and managed (i.e. type, name, description, version, revision, etc.) Depending on the structure applied by the various suppliers, this will apply to software modules, components, elements, etc. Configurable parameters should also be identified and managed.

# SECTION 6 REMOTE CONTROL CENTRES

## 1 General

### 1.1 Objective

This section gives guidance to the technical arrangements in remote control centres (RCC) having the purpose to facilitate remote control and supervision of vessel functions. The objective is to ensure that the remote control and supervision, in combination with automation systems, will provide a level of safety equivalent or better compared to the functions being conventionally controlled and supervised from on-board the vessel.

### 1.2 Scope

#### 1.2.1 Functions

This edition of the guideline covers concepts with remote control and supervision of the navigation and engineering functions, as described in Sec.1 [3]. Remote control and supervision of other functions, e.g. deck/cargo operations and safety functions, are not covered in this edition.

#### 1.2.2 Manning

The guidance covers concepts with or without crew on board the vessel. The guidance is based on personnel in the remote control centre being responsible for operation of the functions provided with remote control.

Manning is not within the scope of class. This guideline does not provide any guidance with respect to number of personnel or competence in the remote control centre, even if these aspects should be analyzed and documented as a part of the concept qualification process, see Sec.3 [2.4.1]. The guidance to the technical arrangements in the remote control centre is based on personnel having roles and responsibilities in accordance with the STCW code. This edition of the guideline is assuming that only the officers of the deck and engineering watch are scope for possible transfer to the RCC. Additional considerations will have to be made for operational concepts based on additional/other roles being covered by personnel in the remote control centre.

#### 1.2.3 Single vessel and control centre

This guidance is based on functions of a single vessel being remotely operated from a single control centre. Additional considerations will have to be made for operational concepts based on remote function operations of several vessels and/or from more than one RCC.

#### 1.2.4 Local jurisdiction

This guideline is not taking into consideration additional regulations that may apply to RCCs because of their location or due to the jurisdiction of regulating authorities. . Regulations resulting from the jurisdiction applicable to the centre should be considered as part of the concept qualification process described in Sec.3 [2].

## 2 Arrangements

### 2.1 Remote control centre

A dedicated physical area should be reserved solely for the tasks necessary to remotely operate the vessel. This area is in the following referred to as the RCC (remote control centre). All remote operations of a vessel's functions should be performed from locations within this RCC.

A RCC is physically detached from the vessel that is controlled, and the RCC may be onshore or onboard another vessel.

This guideline is providing guidance to the technical arrangements in the RCC directly related to remote control and supervision of the vessel functions. The guideline is not covering technical guidance to the centre in general. A standard is intended to be developed by DNV GL for remote operation centres for vessel fleets. Requirements related to general arrangements and provisions of RCCs are intended to be covered by that standard.

## 2.2 Remote workstations

A dedicated physical location in the RCC should be arranged for each of the vessel operational roles covered by personnel in the RCC. These locations will be referred to as remote workstations.

A remote operator should be able to perform the combined tasks of all functions under the responsibility of the role from this workstation.

The remote workstations should be arranged to enable simultaneous performance of tasks under the responsibilities of the different roles covered by the personnel in the RCC without interfering with each other. This should not only take normal operational conditions into consideration, but also emergency conditions and demanding operational situations.

Relevant roles and responsibilities (and accordingly number of workstations), should be part of the safe manning considerations, i.e. in the scope of the concept submitter to propose and the flag administration to approve (see Sec.1 [5.3]).

Even though roles and responsibilities in an RCC may not follow the conventional roles and responsibilities according to the STCW code, this edition of the guideline includes technical guidance to the remote workstation for an officer of a navigational watch in Sec.4 and for an officer of an engineering watch in Sec.5.

## 2.3 Workstation layout

The layout of a remote workstation should enable the officer of the watch to perform the tasks with a reliability and efficiency equivalent to, or better than, when the tasks being performed from a workstation on board the vessel.

DNVGL-RU-SHIP Pt.4 Ch.9 Sec.6 provides requirements for design and arrangements of workstations for the engineering watch. IMO MSC/Circ.982 provides guidance for workstations for the navigation watch. This may be used as a basis for the design and layout of remote workstations, taking additional considerations into account with respect to the tasks being performed from a remote location.

# 3 Hazards and barriers

## 3.1 Hazards

See Sec.4 [1.2] for relevant hazards for the navigation function and Sec.5 [3] for relevant failure modes for systems and components. These apply also with respect to the systems and arrangements in the RCC and form the basis for the technical guidance to the RCC. Additional hazards specific for the RCC should be identified as part of the concept process described in Sec.3 [2]. Examples of relevant hazards may be:

— RCC fire and evacuation
— external power grid black-out
— communication latency and failures
— handover of responsibilities from one operator to another
— unauthorized person(s) accessing the RCC
— unauthorized person(s) accesing the vessel
— cyber attacks, see Sec.7 [4.5].

## 3.2 Redundancy and fault tolerance

Barriers should be arranged towards unwanted events that may affect the capability and availability of remote control and supervision of functions under the responsibility of a remote operator in the RCC.

Relevant hazards as described in [3.1] should be considered, and the systems and equipment in the RCC designed with failure tolerance ensuring that the capability and availability of remote operation will be equivalent to, or better than, when the functions being operated from on board the vessel.

### 3.2.1 Equipment

The guidance given to failures and incidents in Sec.5 [3] applies for equipment in the RCC, as relevant. In addition, the following items should be considered for the RCC:

— Anticipated failures of systems and components located in the RCC, as described in Sec.5 [3], should not result in loss of normal control, supervision and situational awareness of the vessel functions under remote operation from the RCC. Normal operation of the vessel should be maintained as described in Sec.5 [3].
— Potential failures should not prevent the vessel from entering and maintaining the defined MRCs..
— Potential failures should not affect remote manual control, supervision and situational awareness necessary for entering and keeping the vessel in an MRC (for those MRCs depending on remote control and/or supervision).

### 3.2.2 Power supply

Power supply failures in the RCC should be part of the risk assessments. The risk assessments should take into consideration the dependency of the concept on remote control, supervision and situational awareness from the RCC for each of the different MRCs, as well as the concept's ambitions to maintain normal operation in case of failures. In general, the following should apply:

— The internal power supply system in the RCC should be arranged to be redundant in accordance with DNVGL-RU-SHIP Pt.4 Ch.8, with redundant main feeders from the grid and with redundant equipment supplied from separate sections of the system.
— The need for an emergency source of power to ensure continued normal operation from the RCC in case of power grid black-out should be considered, taking into consideration the reliability of the power grid at the location and the concept's ambitions to maintain normal operation.
— A UPS should be arranged to ensure uninterrupted operation of equipment in the RCC in case of grid black-out before emergency or grid power supply is restored. Necessary capacity should be arranged taking into consideration time to restore power supply from an emergency source of power.
— Sufficient emergency lighting should be arranged in the RCC, enabling the personnel to continue watch of the vessel functions.

# 4 Remote situational awareness

## 4.1 General

When personnel in a remote location are responsible for the operation of a function on board a vessel, the remote personnel will need sufficient situational awareness to provide a firm basis for analysing the situation, planning actions and executing remote control of the function.

The situation awareness necessary for the remote operator will depend on the level of automation and decision support functionalities supporting the control of the function. The nature and criticality of the function under control will also influence the required situational awareness. .

## 4.2 Real-time situational awareness

Operation of the function in the remote location should be based on real-time situational awareness for the remote operator. Real-time information should not be based on observations by personnel on board. Therefore, in regard to assisting the remote operator with situational awareness, this guideline is not distinguishing between operational concepts that require personnel on board from those without personnel on board.

However, if response to an event or failure condition is considered not to be time critical, it may be evaluated case-by-case whether the situational awareness for the remote operator may be partly based on information from the on-board personnel. Special considerations should then be made to the reliability of communication and the complexity in describing the condition, event or observation to the remote operator.

## 4.3 Senses

For the remote operation of a function, it should be considered as part of the risk analysis how the different human senses are contributing to the situational awareness for conventional local operation of the specific function. Substitutes for these contributing human senses should be provided by sensor technology, and the information presented to the remote operator in a logical way, ensuring that the total situational awareness for the remote operator will be equivalent to, or better than, compared to the conventional local situational awareness.

### 4.3.1 Sight

Substitutes for the human vision should provide a visual presentation with an update frequency and details sufficient for the remote operator to fully interpret and understand conditions and events relevant for operation of the function.

The quality of visual presentation will depend on the function under remote operation, and may range from a reading to continuous streaming of high definition images with zoom possibilities covering a wide sector. The risk analysis in the concept process described in Sec.3 [2] should for each function under remote control evaluate to what extent the situational awareness necessary for operation of a function is based on visual information.

Further guidance specific for the remote navigation and engineering watches are given in respectively Sec.4 and Sec.5.

### 4.3.2 Hearing

Sounds may form an essential part of the situational awareness for operation of a function, in particular with respect to detection of hazards. In order to ensure an equivalent situational awareness in the RCC, the risk analysis should, for each function under remote control, evaluate to what extent hazards relevant for the function may be detected by sound information.

Substitutes for the human sound perception should be provided where sound contributes to the situational awareness. Suitable technology and necessary performance of the substitute will depend on the function. In general the following should be taken into consideration:

— The substitute should be capable of detecting distinctive sounds relevant for the operation and provide the remote operator with information ensuring that the condition, event or hazard is understood in an equivalent way compared to local sound perception.
— Identification of location/direction of the sound should be provided, as relevant.
— Where microphones with playback to the remote operator are used as part of the sound perception, sufficient noise cancellation properties should be provided to ensure that the distinctive sound relevant for the controlled function can be recognised and understood by the remote operator.

Further guidance specific for the remote navigation and engineering watches are given in respectively Sec.4 and Sec.5.

#### 4.3.3 Other senses

In addition to the sight and hearing, other human senses such as balance and acceleration, smell and temperature, are contributing to the full situational awareness in the control of vessel functions.

The risk analysis should evaluate how the different human senses are contributing to the detection of conditions, events and hazards relevant for each of the functions under remote control, and ensure that the senses are substituted with technology ensuring an equivalent situational awareness for the remote operator. Examples of relevant conditions, events and hazards are:

— vessel movements, including dynamic and static conditions
— ambient conditions, such as reduced visibility (fog, sunset etc.), strong wind, rough sea state, strong currents, heavy precipitation
— explosive and toxic atmospheres
— fire
— high and low temperatures
— vibrations.

#### 4.3.4 Recording and playback of sensor information

It is not expected that a remote operator will continuously monitor all sensor information. In particular the continuous use of headphones is not expected. The sensor information should be continuously recorded with the possibility for simultaneous playback of all relevant sensor information covering a sufficient elapsed time period. Suitable alerts should be arranged to notify the operator upon detection of distinctive sounds relevant for the operation.

# 5 Remote vessel supervision

## 5.1 General

This subsection provides guidance on arrangements in the RCC relevant for remote control and supervision of a vessel. See also Sec.4 and Sec.5 providing guidance specific for remote control and supervision of navigation and engineering functions.

Functions controlled by self-controlling systems (SC) and by decision support systems with conditional execution capabilities (DSE) should be arranged with supervision of the function in the RCC.

The personnel responsible for supervising the operation of a function should have sufficient information about conditions relevant for safe operation of the function and to understand the motivations for the control actions decided by the system.

When such supervision is performed by personnel in a remote location, this may require additional support functionalities in order to analyse and conclude on appropriate control actions compared to supervision of the function from on board the vessel.

## 5.2 Independent supervision

Independent safety systems are to a large extent implemented for certain functions (e.g. machinery functions) to ensure a safe state in case of failures in the automatic control of a function. For other functions that are conventionally operated by humans, the novel technology performing the function control may not be supported by equivalent independent safety systems. This may result in the need for independent human supervision to ensure that the function is performed in a safe way.

When independent supervision of a function is required, the information provided for remote supervision should be sufficient for the remote personnel to do independent analyses of the conditions and make independent conclusions on what the appropriate control actions should be.

Both automatic control and remote supervision of a function are based on sensor data. When independent supervision is required, this supervision should be based on independent sensor information as illustrated in Figure 1. Alternatively, redundant sensor information with cross-verification capabilities or sensors with self-diagnostic capabilities may be considered.

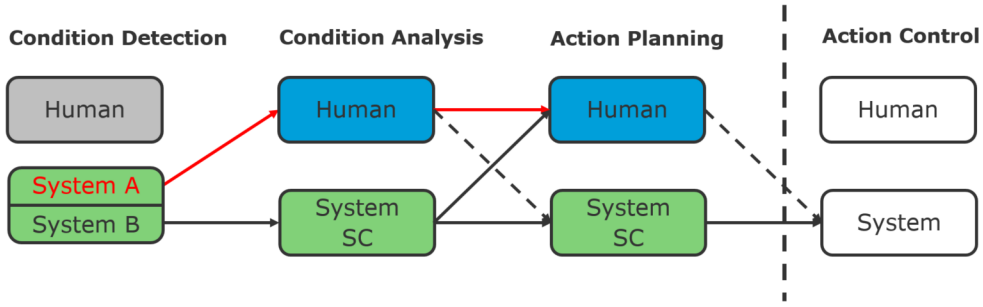


**Figure 1 Independent supervision**

The risk analysis to be performed as part of the concept process described in Sec.3 [2] should include analysis of the functions under the responsibility of remote operation from the RCC, and consider the need for independent remote supervision in order to obtain an equivalent safety level compared to conventional operation of the function.

## 5.3 Intended action control and pre-warning

Systems with self-controlling capabilities (SC) and decision support systems with conditional execution capabilities (DSE) should provide information to the remote operator about intended control actions in time for the remote operator to analyse the situation, assess the intended control actions and intervene, if required.

Remote operators should be informed about hazards and developing conditions in time to analyse the situation, plan appropriate control actions and intervene before a situation becomes critical. Sufficient pre-warnings and caution alerts should be provided for this purpose.

## 5.4 Alert management

Alert management should be consistent in the RCC. All navigation related alerts should be managed in accordance with the BAM concept of IMO as defined in MSC.302(87). Alert management should be implemented in a corresponding way for other functions under remote operation from the RCC. See also Sec.5 [6.4.2] for alert management related to engineering functions.

Alarms should only be used when actions are required and should clearly indicate required action.

Alerts to a specific role should only be given on the related workstation. Common alerts may be given on several workstations. Preferably, alarms should not be common, and instead should be given only to the role responsible for the required action.

## 5.5 Functional status

Systems and components supporting functions under remote operation should be subject to an initial test prior to each voyage. This initial function test should include switching between redundant systems and components in order to disclose hidden failures or malfunctions before departure. A corresponding function test should be possible to initiate throughout the voyage, e.g. before entering critical operational situations.

The remote workstation should be arranged with sufficient overview of the condition of all the functions under the responsibility of the remote operator throughout the voyage. This overview should be displayed at all times and presented in such a way that the remote operator in a simple and unambiguous way will have a full understanding of the status of all the functions.

This may be presented in three levels for each function:

- green: the function or system is operational at full capacity, including any redundancy and health condition of supporting systems
- yellow: the function or system is operational, but not at 100%. It may have lost some capacity, functionality or redundancy. It should be possible for the operator to easily obtain detailed information about the current limitations
- red: the function or system is unable to fulfil its intended purpose.

For functions being provided with different modes of control (e.g. M, DSE or SC), the mode of control for each function should be displayed at all times.

## 5.6 Consequence analysis and decision support

In case of abnormal conditions, such as deteriorating weather conditions or failures affecting the redundancy, the remote operator should be provided with sufficient information to analyse the situation and decide on appropriate actions.

Considering that the analysis and evaluations are performed from a remote location, the remote operator should be aided by decision support functions in analysing potential risks and consequences of continued operation in the abnormal condition. The level of decision support necessary should be based on the complexity and criticality of the function, the objective to be achieved, and an equivalent basis for making decisions compared to onboard analysis of the situation. A consequence analysis may be necessary to help identify the level of decision support needed.

Remote operators should not need to review operation manuals from manufacturers for how to remotely handle abnormal conditions. Instructions on how to sequentially restore functions or how to operate the equipment / functions during extreme conditions should, to the furthest extent, be covered by decision support functionalities or automation.

## 5.7 Contingency plans and MRCs

See Sec.4 [6] for guidance regarding contingency plans.

The contingency plan should be displayed at all times in the RCC, providing continuous information about viable MRCs throughout the voyage. Given that a vessel may have several viable MRCs depending on the location and on the failure which may occur, a consequence analysis or other on-line tools should be implemented to inform the operator in RCC about the MRC which will at any time be automatically initiated upon loss of communication with RCC.

Personnel in the RCC should be able to select and initiate any viable MRC at any time throughout the voyage. Such orders should have the highest priority. This entails that a system controlling the vessel in an MRC should follow new orders in case a new MRC is selected in the RCC.

## 5.8 Data logging

In order to support failure and incident analysis as well as planning of mainenance, data related to key vessel functions should be electronically logged and stored. The information should be available to personnel in a RCC.

The following should as a minimum be logged:

- operational status of key vessel functions including communication links
- alerts
- manual orders
- all data input and output to/from decision support and automation systems.

If records are stored on board an alert should be given in due time before storage capacity is exceeded. To avoid loss of information, it should be possible to transfer the records to a database on shore.

The responsible engineering watch should use electronic engine logbooks. The objective is to efficiently share information between personnel on the vessel and in RCC, as well as providing a basis for analysis and continuous improvement.

All nodes in the autoremote infrastructure should be synchronized to attain a uniform time tagging of alerts and a proper sequential logging.

# SECTION 7 COMMUNICATION FUNCTIONS

## 1 Purpose

Communication plays an important role in most autoremote concepts and systems. This section provides guidance regarding functionality and cyber security of the communication to and from the vessel.

## 2 Hazards

At least the following incidents and failures should be included when performing a risk analysis of the communication systems and functions:

— unauthorized persons gaining access to the communication link
— jamming of wireless communication links
— interception of data traffic by 3rd party
— spoofing of data by 3rd party
— malware entering the systems
— failure of electronic components in the communication links
— less than ideal radio-coverage for wireless links
— error in transmission of data (also known as bit-faults)
— lack of acknowledgement of command(s)
— wrong configuration of communication functions
— unexpected reduction of available bandwidth during operations
— unexpected increase of latency during operations
— unstable data-links over time
— network storms
— loss of power.

## 3 Baseline

The following requirements are valid for a conventional vessel:

— Internal vessel communication (between personnel).

  Compliance with SOLAS III/6 is expected. In addition, voice communication with on board / on deck personnel may be required as part of docking operations.

— External communication.

  Compliance with SOLAS IV/4 *Radiocommunications - functional requirements* is expected.

## 4 Autoremote vessels

### 4.1 Vessel data communication with RCC

#### 4.1.1 General

The communication link between the ship and a remote control centre (RCC) should be available, secure and capable of supporting the intended use. The more responsibility the RCC has for the operation of vessel functions, the more available, robust and secure the communication link needs to be.

Coverage-analysis of the different wireless communication solutions must be performed for each concept qualification project in order to determine the suitability of a specific solution or technology.

The aspects listed below serves as the basic guidance for any communication link between the ship and a remote control or monitoring center:

— The maximum bandwidth required should be calculated and documented. The calculation should consider the worst case scenario based on the intended use, e.g. where real-time transmission of sensor-data from multiple sensors like video-cameras, images, radar-information, audio, etc. is transmitted and received at the same time.
— The actual latency requirements (based in the intended use) should be calculated and specified.
— The communication between the ship and the RCC should be monitored so that the on-board system and the RCC independently will detect a loss of communication within a reasonably time.
— A cyber-security analysis should be performed on the total communication system, including the ship-systems, the datalink, and the remote control centre (see [4.5]).
— All interfaces and protocols used in the communication link should be specified and described.

### 4.1.2 Communication for control of vessel key functions

If the remote control center (RCC) is responsible for the control of any of the vessel key functions (see Sec.2 [6]), the availability, reliability, flexibility and robustness is expected to be high; and the monitoring of the link to be comprehensive. In addition to the guidance in [4.1.1], the following aspects should be observed:

— The actual latency between the vessel and the RCC should be monitored so that the on-board system and the RCC independently will detect if the latency exceeds the specified maximum.
— The communication link should be fault-tolerant so that it can operate at 100% capacity even with a single component-failure.
— The communication link should consist of at least two independent communication channels, preferably using different underlying technologies and suppliers.
— If the actual bandwidth or latency performance is lower than the required levels, alarms should be given to the operator.
— It should be possible to prioritize specific communication types to secure that the most important communication types are prioritized if there is insufficient bandwidth (see [4.1.3]).
— The operator should be able to seamlessly switch all data between the different channels without any negative effect on the operations.
— The operator should be able to configure the channels so that different channels carry only parts of the total data-stream at the same time (e.g. imagery and radar on one channel, the rest on another).
— The operator should be able to test and diagnose all functionality and characteristics of one communication channel while the other(s) are used for actual operations.
— The communication should be recorded.
— The network components on-board and in the RCC should be type-approved according with DNVGL-CP-0231 *Type approval programme for cyber security*.
— The status and events related to the communication link shall be logged so that they can analyzed at a later stage (see Sec.6 [5.8]).

### 4.1.3 Information priority

In case of insufficient bandwidth between the vessel and the remote control centre, the data types should be prioritized in the following order (highest priority first):

1) emergency control (e.g. MRC activation)
2) remote control commands (including data) for key vessel functions
3) situational awareness data for remote control of key vessel functions
4) supervision data
5) maintenance data.

## 4.2 Vessel communication with off-ship systems and sensors

### 4.2.1 Communication for operational purposes

If vessel key functions are depending on ship systems having access to off-ship systems and sensors to execute relevant functions, the communication link between the vessel and these systems/sensors should follow the guidance in [4.1.2].

Examples of off-ship systems and sensors are:

— shore-based radar
— weather forecast service
— automated VTS communication
— shore-based cameras (e.g. for docking operations).

### 4.2.2 Communication for maintenance

When communication is needed in order to perform maintenance on ship systems, the communication should not be possible without prior approval per case by either personnel on board or by the remote control centre.

If the maintenance is performed when the ship is operating, the communication link should follow the guidance in [4.1.2].

## 4.3 Vessel external communications

When the navigation functions are under responsibility of remote operation from the RCC, the autoremote infrastructure will still need to be able to communicate with external stakeholders to the ship.

This means that the following functions need to be taken care of, either by relaying the task to personnel in the RCC, or by automatic systems on board:

— Communicating with other vessels, VTS, tugs, pilot station, etc. using VHF transmitter on board the vessel.
— Transmit emergency messages from the vessel.
— Relay emergency messages received by the vessel.
— Reply to messages from other vessels.
— Interpret sound and light signals around the vessel and recognise day shapes and navigation lights (e.g. vessels not under command).
— Voice communication with crew and passengers on board the vessel.
— Voice communication with humans near the vessel.

## 4.4 RCC communication with external stakeholders

The RCC personnel should be able to reliably and securely communicate with external stakeholders like the emergency services, VTS, pilot, tug-boat operators etc. using communication means that are not depending on the communication link between the RCC and the vessel.

## 4.5 Cyber security

The vessel should have DNV GL class notation **Cyber secure(Advanced)**.

Alternatively, cyber-security assessments should be performed on the total system (including the on-board systems, the datalink, and the RCC) and all resulting mitigation-actions should be implemented and verified. Refence is given to DNV GL recommended practice DNVGL-RP-0496 which describes three levels of assessment:

1) high level assessment
2) focused assessment

3) comprehensive, in depth assessment.

For the purpose of analysing autoremote systems, level 2 and 3 are recommended.

Regardless of the results from the cyber-security assessments, the following items should be observed:

— All parts of the operation of cyber systems for autoremote vessels should be governed by an up-to-date cyber security management framework which includes necessary policies, procedures and technical requirements.
— Incidents related to cyber security should be prevented or mitigated by applying a recognised framework, e.g. based on the IEC 62443 series of standards or the NIST cybersecurity framework.
— Any personnel who shall access systems or locations relevant for autoremote vessels should be informed/ trained on relevant security policies. It is widely recognised that lack of awareness is a major cause of cyber security incidents.
— Any system or component used for communicating information to shore or to other vessels should be type approved in accordance with DNVGL-CP-0231.
— Network segmentation should be applied as stated in Sec.5 [6.5]. The methods of network segmentation should include as relevant the use of air-gap, firewalls, DMZ, VLAN and/or layer 3 network devices.
— Malware protection should be implemented as needed and feasible to prevent spreading between different systems or network segments.
— Software-based components should be regularly analysed from a security point of view, and if applicable kept updated to block known threats and vulnerabilities.

# APPENDIX A LIST OF POTENTIAL MINIMUM RISK CONDITIONS

The minimum risk conditions (MRCs) for an autonomous or remotely operated ship depend on many aspects, for example the ship's functionality, the manning, it's location and the current weather.

Below is a list of possible MRCs that may be applicable. However, the MRCs that should be included in the operation of a specific ship needs to be decided based on thorough case-by-case analysis. This list below is not exhaustive, it is only intended to give examples and serve as inspiration when defining MRCs for a specific ship (see the description of the MRC concept in Sec.2 [5]).

Potential MRCs:

1) Stay moored at quay: may be applicable for many events and failures that takes place while the ship is still alongside the quay.
2) Move away from the quay and other vessels: especially relevant if the ship has caught fire or if there is a fire in close vicinity of the ship.
3) Limp home: only relevant if the ship still has some propulsion, steering, and navigational functionality left. Limping' may be defined as a limited speed, rudimentary anti-collision functionality and turning on the "not under command" signal lights. 'home' should be a pre-defined place.
4) Move as slowly as possible: if the ship does not have position-keeping capabilities, but still has some outlook, propulsion and steering, it may move slowly without posing a danger to others, the environment, or itself. This may give the operator(s) and systems time to rectify the situation.
5) Navigate to next waypoint and stop there: may typically be applied if the event leading to the MRC is failure of a secondary function or system.
6) Call for assistance (tug): in addition to calling for assistance, the ship normally need to provide some means for other ships (typically tugs) to fasten tow, e.g. by extending towing lines.
7) Drop (emergency) anchor: may be used if the water-depth is within a suitable range. If used as a 'last resort MRC', the anchoring system will typically need an independent power supply.
8) : maybe one of the more extreme MRCs, and requires that suitable beaching zones have been identified up front. This MRC may typically be used when energy reserves are about to become depleted.
9) Keep position: may typically be used if the data-link to the remote-control centre is lost, but requires considerations regarding the current waters and the position of the ship, e.g. when navigating narrow straits. This MRC comes in two variants:
    1) If moving, stop and keep position.
    2) If stationary, stay at current position.
10) Abort current operation (e.g. hoisting, loading, fuelling, charging): the operation in question should be aborted. It should be defined if the operation should just 'freeze' where it is, or if it should continue/ reverse to some pre-defined state.

# APPENDIX B LIST OF POTENTIAL AUTOREMOTE FUNCTIONS

The sub-chapters below list functions associated with a traditional ship that may be subject to a high level of automation and remote control.

The list is not exhaustive, but indicates the abstraction-level normally applied for this kind of deliberations.

## 1 Navigation functions

- Voyage planning
- Route planning
- Determine ship position, course and speed
- Follow route
- Keep general lookout
- Determine CPA and TCPA for potential navigational dangers/objects and other ships
- Monitor depth, sea-state, tide, current, weather and visibility
- Monitor seakeeping performance
- Monitor for, and react to, distress signals from other seafarers
- Determine the situational mode (e.g. unrestricted, dense traffic, costal navigation, narrow passage, restricted visibility, heavy weather, very cold weather, ice conditions, pilot required)
- Docking
- Undocking
- Manoeuvring
- Propulsion control
- Steering
- Grounding and collision avoidance
- Weather routing
- Communication with other vessels
- Communication with shore (e.g. notice to mariners, vessel traffic service, weather forecast, rescue services, pilot services, etc)
- Navigation lights and sound signals
- Overall supervision of bridge-related systems
- Overall supervision of own ship's state and operational capabilities

## 2 Engineering functions

- Overall supervision of machinery-related systems
- Machinery control and monitoring (including auxiliary functions like fuel, cooling, heating lube-oil, air, hydraulics, pneumatics etc. as needed)
- Electrical Power generation and distribution
- Fuel optimization
- Emission control and monitoring
- Fuel management
- Battery charging control and monitoring
- Maintenance planning

## 3 Other vessel functions

- Loading of cargo
- Discharging of cargo
- Monitoring of cargo

— Shell-door control and monitoring
— Watertight doors control and monitoring
— Stability/ballast control and monitoring
— Ballast water control and monitoring
— Bilge and drainage control and monitoring
— HVAC control and monitoring
— Freshwater control and monitoring
— Anchoring
— Mooring
— Unmooring
— Fire detection
— Fire fighting
— Logging of data and events

## 4 Special operations

— Position keeping (dynamic positioning)
— Seabed mapping
— Fire-fighting
— Rescue operations
— Damage control

# APPENDIX C NAVIGATION SYSTEMS - APPLICABILITY OF CONVENTIONAL CARRIAGE REQUIREMENTS FOR AUTOREMOTE VESSELS

## 1 General

The intention with this part is to give an overview of systems currently required to be carried by conventional vessels, including applicable performance standards for these systems, and DNV GL's point of view regarding the need for these systems in remotely operated- and autonomous vessels.

For conventional vessels, the carriage requirements for navigational systems are covered by SOLAS V/19, 19-1 and 20.

For high-speed crafts the 2000 HSC Code in its entirety can be used to cover SOLAS. The carriage requirements for navigational equipment is covered by Ch.13.

All navigational equipment installed, including required and additional equipment, should be of a type approved by the administration according to the applicable performance standards for the equipment - ref. SOLAS V/18 and 2000 HSC Ch.13.17.

## 2 Carriage requirements for SOLAS V and 2000 HSC Code and relevance for autoremote vessels

### 2.1 Heading information systems and tools

#### 2.1.1 Magnetic compass - IMO Res. A.382(X)

— Standard magnetic compass applicable for all ships irrespective of size. For HSC a magnetic compass suitable for the speed and motion of the craft is required.
— The intention with the magnetic compass is a method for determination of the ship's heading that is independent of any power supply. The magnetic compass is designed to seek a certain direction in azimuth and to hold that direction permanently, and which depends, for its directional properties, upon the magnetism of the earth.
— The requirement for a heading information system not dependent of power is assumed unnecessary on remotely operated- and autonomous vessels.

#### 2.1.2 Spare magnetic compass - IMO Res. A.382(X)

— Applicable for all ships irrespective of size.
— According to IMO MSC/Circ.1224 a second gyro compass may fulfil this requirement. A redundant heading information system is deemed necessary for remotely operated - and autonomous vessels.

#### 2.1.3 Transmitting heading device (THD) – ref. IMO Res. MSC.116(73)

— Applicable for ships above 300 GT and passenger HSC certified to carry 100 passengers or less. A GNSS based THD is applicable for compliance with the Polar Code on latitudes above 80 degrees N/S.
— The THD should provide heading information about the ship's true heading to systems which require this information and may be based different types of sensing methods like magnetic, gyroscopic and GNSS.
— A redundant electronic heading information system is assumed as major input to the NDSS CA-GA; hence a THD may be part of this for remotely operated- and autonomous vessels.

#### 2.1.4 Gyro compass – ref. IMO Res. A.424(XI) (Ships) /A.821(19) (HSC)

— Applicable for ships above 500 GT, HSC certified to carry more than 100 passengers and cargo HSC.
— The gyro compass should provide self-contained, non-magnetic heading information in relation to geographic (true) north.

— As written for THD a redundant electronic heading information system is assumed as major input to the NDSS CA-GA. Due the independence from sources external to the vessel it is assumed that gyro compass information will be required as the main source of heading information.

### 2.1.5 Pelorus or compass bearing device – ref. IMO Res.A382(X)/ISO 25862:2009

— Applicable for all ships irrespective of size.
— The pelorus is an optical device used to cover the requirement to take relative bearings over the horizon of 360 degrees.
— It is assumed that a camera based system interconnected with the heading information system and able to take bearings, will be required for remotely operated – and autonomous vessels.

### 2.1.6 Bearing repeater SOLAS V/19

— Applicable for ships above 500 GT however ships less than 1600 GT shall be fitted as far as possible.
— The intended use of the bearing repeater is to take true visual bearings, over an arc of the horizon of 360 degrees using the gyro compass as heading source.
— As for the pelorus it is assumed that a camera based system interconnected with the heading information system and able to take bearings, will be required for remotely operated – and autonomous vessels.

### 2.1.7 Means of correcting heading and bearings to true at all times

— Applicable for all ships irrespective of size.
— This requirement is based on the need for deviation tables used to correct magnetic headings and bearings. Assumed unnecessary on remotely operated- and autonomous vessels without magnetic compass.

### 2.1.8 Nautical charts – SOLAS V/19

— Applicable for all ships irrespective of size and HSC.
— This requirement cover nautical charts and nautical publications to plan and display the ship's route for the intended voyage and to plot and monitor positions throughout the voyage.

### 2.1.9 Electronic Chart Display and Information System (ECDIS) – ref. IMO Res. MSC.232(82)

— Applicable for passenger ships above 500 GT, cargo ships above 3000 GT and HSC.
— The primary function of the ECDIS is to contribute to safe navigation by reducing the navigational workload for the OOW compared with paper charts. ECDIS will cover the requirements for nautical charts if approved ENCs and adequate back-up arrangements are provided.
— An ECDIS using approved ENCs is assumed to form the basis, or being a major part, for anti-grounding in a Navigation Decision Support system for Collision- and Grounding Avoidance – NDSS CA-GA and hence assumed required for remotely operated- and autonomous vessels.

### 2.1.10 Back-up arrangements to ECDIS - ref. IMO Res. MSC.232(82)

— Applicable for all ships irrespective of size where ECDIS is required or if ECDIS is used to cover the chart requirements.
— The purpose of an ECDIS back-up system is to ensure that safe navigation is not compromised in the event of ECDIS failure. This should include a timely transfer to the back-up system during critical navigation situations. The back-up system shall allow the vessel to be navigated safely until the termination of the voyage.
— Back-up arrangements may be either up-to-date paper charts, a type approved electronic back-up ECDIS or a second independent ECDIS.
— As a chart system is forming the major part of NDSS CA-GA, electronic back-up arrangements should be available for remotely operated- and autonomous vessels.

### 2.1.11 Electronic position fixing system (EPFS) – ref. IMO Res. A.1046(27)

— Applicable for all ships irrespective of size and HSC.

— SOLAS and the 2000 HSC Code describe a global satellite navigation system – GNSS or a terrestrial radio navigation system suitable for the operational area and forms the main position input to the ECDIS. No electronic back-up is described.
— Where a radio navigation system is used to assist in the navigation of ships in ocean waters, the system should provide positional information with an error not greater than 100 m with a probability of 95%.
— Where a radio navigation system is used to assist in the navigation of ships in harbour entrances harbour approaches and coastal waters, the system should provide positional information with an error not greater than 10 m with a probability of 95%.
— For remotely operated - and autonomous vessels a redundant position fixing system able to give input of position and timing information is assumed necessary. In addition, we assume that at least two separate methods for position determination should be part of the system where GNSS seems like the most suitable main method.

### 2.1.12 Radar reflector – ref. IMO Res. A.384(X)

— Applicable for ships below 150 GT.
— The radar reflector shall enhance the radar return and thus to improve the ship's visibility to radar with an adequate polar diagram in azimuth, and an echoing area:
  — preferably, of at least 10 m, mounted at a minimum height of 4 m above water level; or
  — if this is not practicable, of at least 40 m, mounted at a minimum height of 2 m above water level.
— Smaller remotely operated- and autonomous vessels, and in particular those made of glass reinforced plastic, may be required to be equipped with a radar reflector.

### 2.1.13 Sound reception system (SRS) – ref. MSC.86(70) Annex 1

— Applicable for all ships with enclosed bridge wings.
— Sound reception systems are acoustical electronic navigational aids to enable the officer of the watch to hear outside sound signals inside a totally enclosed bridge in order to perform the look-out function as required in the International Regulations for Preventing Collisions at Sea, 1972.
— A SRS is assumed applicable for remotely operated- and autonomous vessels in order to get full situational awareness.

### 2.1.14 Communication to emergency steering position - SOLAS V/19 and HSC 2000/5.4.2

— Applicable for all ships where an emergency steering position is provided.
— For remotely operated and autonomous vessels it is assumed that additional system redundancy should be included in the steering control system.

### 2.1.15 Daylight signalling lamp – ref. IMO MSC.95(72)

— Applicable for ships above 150 GT
— The objective of daylight signalling lamps is to convey information between ships, or between ship and shore, by means of light signals, both by day and by night. This is not necessarily a safety critical system when there are other methods for ship-ship communication; hence for remotely operated- and autonomous vessels other methods like VHF/GMDSS and through the AIS message terminal may be used.
— Remote operation of the daylight signalling lamp from the RCC is also possible.

### 2.1.16 Bridge Navigational Watch Alarm System – BNWAS – ref. IMO MSC.128(75)

— Applicable for ships above 150 GT.
— The purpose of the BNWAS is to monitor bridge activity and detect operator disability which could lead to marine accidents. The system monitors the awareness of the Officer of the Watch (OOW) and automatically alerts the Master or another qualified OOW if for any reason the OOW becomes incapable of performing the OOW's duties.
— Based on the above intention for manned vessels a system with similar functionality should be provide for any land based control stations.

### 2.1.17 Echo sounder - IMO Res.A224(VII) as amended by Annex 4 to Res. MSC74(69)

- Applicable for ships above 300 GT and non-amphibious HSC.
- The echo sounder should provide reliable information on the depth of water under a ship to aid navigation.
- Echo sounder for measuring the depth under the keel may be an important input to a NDSS CA-GA for remotely operated- and autonomous vessels.

### 2.1.18 Speed and distance measuring devices IMO Res. A.824(19)

- Speed and distance through the water
  - Applicable for ships above 300 GT and HSC for input to the radar. It is assumed that this will also be applicable for remotely operated- and autonomous vessels.
- Speed and distance over the ground
  - Applicable for ships above 50.000 GT.
  - Accurate speed over ground is especially important as part of the docking operations for larger vessels since even low relative speed to a fixed installation may cause extensive damage to both ship and the installation. For remotely operated- and autonomous it is assumed that this is important even for smaller vessels. There may however be solutions that are more specialized towards the different parts of the operations.

### 2.1.19 Automatic Identification System - AIS - ref. IMO MSC.74(69) Annex 3

- Applicable for ships above 300 GT on international voyages, all ships above 500 GT, all passenger vessels and all HSC.
- The Automatic Identification System, AIS, is an autonomous and continuous vessel identification system used for safety and security of maritime and inland waterway areas. It allows vessels to electronically exchange with other nearby ships and provide authorities ashore with the vessel identification data, position, course and speed.
- As AIS presently is the only approved ship-ship communication system that automatically communicate with other vessels it is assumed as a major input to the NDSS CA-GA for communication of own and surrounding ships' static and dynamic data for use in anti-collision and for classification purposes.

### 2.1.20 Gyro compass - ref. IMO Res. A.424(XI)

- Applicable for ships above 500 GT, HSC certified to carry more than 100 passengers and cargo HSC.
- The gyro compass should provide self-contained, non-magnetic heading information in relation to geographic (true) north.
- As written for THD a redundant electronic heading information system is assumed as major input to the NDSS CA-GA. Due the independence from sources external to the vessel it is assumed that gyro compass information will be required as the main source of heading information.

### 2.1.21 Rudder, propeller, thrust, pitch and operational mode indicators

- Applicable for ships above 500 GT and HSC.
- Intention is to determine and display rudder angle, propeller revolutions, the force and direction of thrust and, if applicable, the force and direction of lateral thrust and the pitch and operational mode, all to be readable from the conning position.
- Assumed covered by redundant sensors on remotely controlled- and autonomous vessels.

### 2.1.22 Radar equipment – ref. MSC.192(79)

#### 2.1.22.1 General

In general the radar equipment should assist in safe navigation and in avoiding collision by providing an indication, in relation to own ship, of the position of other surface craft, obstructions and hazards, navigation objects and shorelines.

For this purpose, radar should provide the integration and display of radar video, target tracking information, positional data derived from own ship's position (EPFS) and geo referenced data. The integration and display of AIS information should be provided to complement radar. The capability of displaying selected parts of Electronic Navigation Charts and other vector chart information may be provided to aid navigation and for position monitoring.

The radar, combined with other sensor or reported information (e.g. AIS), should improve the safety of navigation by assisting in the efficient navigation of ships and protection of the environment by satisfying the following functional requirements:

— in coastal navigation and harbour approaches, by giving a clear indication of land and other fixed hazards;
— as a means to provide an enhanced traffic image and improved situation awareness
— in a ship-to-ship mode for aiding collision avoidance of both detected and reported hazards; - in the detection of small floating and fixed hazards, for collision avoidance and the safety of own ship; and
— in the detection of floating and fixed aids to navigation

#### 2.1.22.2 X-band radar

— Applicable for ships above 300 GT and HSC.
— The X-band radar is today the only on-board system for receiving information from search and rescue transponders solely based on radar; hence presently it is assumed that if a remotely controlled- or autonomous vessel shall take part in search- and rescue operations then a type approved X-band radar is required. Note that an AIS-SART is an available system that will give similar information; hence for future applications the need for X-band radar to detect SARTs may be reduced.

#### 2.1.22.3 S-band radar

— Applicable for ships above 3000 GT, HSC above 500 GT and passenger HSC certified to carry more than 450 passengers.
— The S-band radar will have better performance in demanding weather conditions where the X-band radar have risk of high clutter density. The use of X-band instead may however be accepted by the administration when considered appropriate. The need on remotely operated- and autonomous vessels therefore is closely linked with the CONOPS of the vessel and if other radar applications may cover the redundancy aspect.

#### 2.1.22.4 Electronic plotting aid (EPA)

— Applicable for ships above 300 GT.
— Covered radar equipment CAT 3 for manual direct plotting.
— Covered by radar equipment CAT 2 and 1.
— Assumed inadequate to cover needed plotting capabilities for remotely controlled- and autonomous vessels

#### 2.1.22.5 Automatic tracking aid (ATA)

— Applicable for ships above 500 GT and HSC.
— Covered by radar equipment CAT 2.
— The radars used on remotely controlled- and autonomous vessels should be equipped with facilities for automatic acquisition and tracking of other vessels. Setting up the radar to avoid land may be correlated with the chart function in the NDSS CA-GA.

#### 2.1.22.6 Automatic radar plotting aid (ARPA)

— Applicable for ships and HSC above 10.000 GT.
— The radars used on remote- and autonomous vessels should be equipped with facilities for automatic acquisition and tracking of other vessels. Setting up the radar to avoid land may be correlated with the chart function in the NDSS CA-GA

### 2.1.23 Heading or track control system (HCS/TCS)– ref. IMO Res. MSC.64(67) Annex 3 and MSC.74(69) Annex 2

— Applicable for ships above 10.000 GT and HSC.
— Within limits related to the ships' s manoeuvrability the heading control system, in conjunction with its source of heading information, should enable a ship to keep a preset heading with minimum operation of the ship' s steering gear.
— Track control systems in conjunction with their sources of position, heading and speed information are intended to keep a ship automatically on a pre-planned track over ground under various conditions and within the limits related to the ship's manoeuvrability. A track control system may additionally include heading control.
— A track controls system is assumed a major input or part of the NDSS CA-GA for remotely operated- and autonomous vessels.

### 2.1.24 Rate-of-turn indicator (ROTI) - ref. IMO Res. A.526(13)

— Applicable for ships above 50.000 GT and HSC above 500 GT.
— The ROTI should be capable of indicating rates of turn to starboard and to port of the ship to which it is fitted. It may be a self-contained unit; alternatively it may form part of, or derive information from, any other appropriate equipment.
— Rate-of-turn information is assumed important in the NDSS CA-GA for remotely operated- and autonomous vessels; however this information may typically be received from the heading information system; hence the need for indication of rate-of-turn information may be part of the system for situational awareness for a shore-based control and monitoring centre.

### 2.1.25 Long-range identification and tracking of ships (LRIT)

— Applicable for most vessels engaged on international voyages. LRIT is in short, a surveillance/security tool for Flag states to have control on the movements of international shipping.
— Initially remote operated and autonomous vessels are assumed not to perform international voyages; hence LRIT is assumed not required for such ships in the near future. For local authorities to gain control of ship movements, the use of AIS will most probably be the preferred tool.

### 2.1.26 Voyage data recorder (VDR) – IMO MSC.333(90)

— Applicable for all passenger vessels and cargo ships/HSC above 3000 GT.
— In general, the purpose of the VDR is to maintain a store, in a secure and retrievable form, of information concerning the position, movement, physical status, command and control of a ship over the period leading up to and following an incident having an impact thereon.
— A VDR or a system with similar functionality covering both the ship and the control centre is assumed required for remotely controlled- and autonomous vessels.

### 2.1.27 Night vision equipment – ref. IMO MSC.94(72)

— Applicable for HSC where operational conditions justify the provision of night vision equipment.
— Night vision equipment facilitates the detection at night of hazards to navigation above the water surface, thus providing essential information to the navigator for collision avoidance and safe navigation of High-Speed Craft. Typical hazards to HSC include, for example, small unlit boats, floating logs, oil drums, containers, buoys, ice, hazardous waves and whales.
— The use of night vision equipment for remotely controlled- and autonomous vessels is assumed important as part of an optical system for detection and classification of hazards to navigation.

### 2.1.28 Searchlight for high speed craft – ref. MSC.97(73)/ISO 17884

— Applicable for all HSC.
— At night, searchlights shall be capable of locating objects within a sufficient distance from one's own craft. The searchlights shall be provided with an electrical, hydraulic or pneumatic remote control for pan and tilt movement.

— Based on the CONOPS the total amount of equipment provided for detection and classification of hazards to navigation, the use of searchlights may be a complement to the night vision equipment for remotely controlled- and autonomous vessels.

# APPENDIX D NAVIGATION SYSTEMS - ADDITIONAL SYSTEMS FOR AUTOREMOTE VESSELS

## 1 General

This section contains equipment for vessels where the navigation function is fully covered by remote or automatic functions. functions. When only partially remote or automatic functions are used, some of the systems described below may be used in order to either cover or enhance the functions required for safe manning of a vessel. The principle is to achieve full operational awareness of the location of the vessel and its surroundings.

## 2 Certification

All equipment installed should be compliant with related IMO performance standards. In the case where appropriate performance standards have not yet been developed, compliance with IMO recommendations on general requirements for GMDSS and electronic navigational aids - resolution A.694(17) - and the appurtenant test standard IEC 60945 or similar should be the minimum applied.

For demonstration of compliance, the equipment should be evaluated as part of the technology qualification process as described in Sec.3.3; hence be type approved or case-by-case approved and a certificate of compliance should have been issued. Additional functionality requested by these recommendations but not forming a part of the performance standards should be tested for compliance with the functionality of these recommendations.

## 3 Systems

### 3.1 Steering control

There should be two separate and independent steering control systems for all applications where steering is needed to get to a MRC. In such systems, one system should be able to take over command in case of failure of the other system.

### 3.2 Heading information systems

#### 3.2.1 Main compass system

Minimum two separate, independent and self-contained heading information systems for determination of the ship's heading in relation to geographic (true) north should be provided.

#### 3.2.2 Distribution system

The distribution system of heading information should enable continuous distribution of heading information to systems dependent on this. Applicable systems include the navigation decision support system for collision- and grounding avoidance (NDSS CA-GA).

### 3.3 Speed information systems

#### 3.3.1 Speed through water

A speed log, or other approved means, for measuring the ship’s speed and distance through the water (STW) continuously should be provided. The system should be able to support uninterrupted output of STW to the radars also when other speed modes are selectable (e.g. SOG).

### 3.3.2 Speed over ground

A speed log, or other approved means, for measuring the ship's speed over ground (SOG) in both longitudinal and transversal (athwart ship) directions should be provided.

## 3.4 Collision avoidance -decision support systems

### 3.4.1 Radar detection

The ship should as a minimum be provided with one azimuth-stabilized radar operating in the X-band (9 GHz). Additional near-ship radar(s)and/or other detection technologies should be provided for safety and manoeuvring purposes.

### 3.4.2 Automatic identification

The ship should be equipped with an automatic identification system (AIS). This system should be interconnected with the radars and ECDIS's assisting in target detection, classification and identification and forming a part in the total collision and grounding avoidance system.

It must however be taken into account that AIS information is highly susceptible to jamming, spoofing and human error and therefore needs to be managed accordingly.

### 3.4.3 Sound reception

A sound reception system capable of detecting sound signals from ship whistles operating according to COLREG Annex III should be provided.

### 3.4.4 Visual target detection and classification

A system for visual target detection and classification should be provided. The system should as a minimum cover the following functions:

- Lookout function during day- and night-time
  - Night vision capabilities similar to or better than as specified in the *International Code of Safety for High-Speed Craft*, 2000 (2000 HSC Code)
- Detect objects above the water's surface and process the results in real time
- Taking visual bearings in relation to geographic north and input of these to a system for position determination. Performance should be i.a.w. bearing device requirements.
- Stabilised in pitch, yaw and roll
- Optical zoom
- Clear view arrangements including wiper, fresh water washing and heating (in temperatures below 0°C.

## 3.5 Grounding avoidance – decision support systems

### 3.5.1 Chart information

An ECDIS or another approved system for reading of electronic navigational charts (ENC) with appropriate accuracy (see Sec.4 [3.1.2.3]) should form the basis for a safe planning and execution of a voyage plan.

### 3.5.2 Track control

A track control system able to execute and deviate from the voyage plan should be provided.

### 3.5.3 Electronic position fixing

Minimum two separate and independent electronic position fixing systems (EPFS) based on different technologies, both suitable for the area of operations should be part of the grounding avoidance system.

### 3.5.4 Depth measuring

A system for measuring the depth under the keel should be provided.

## 3.6 Weather surveillance and vessel monitoring

A system for determination of local weather and the influence this may have on the ship and a system for monitoring of ship movements and hull stress should be provided.

## 3.7 Navigation Decision Support system for Collision- and Grounding Avoidance – NDSS CA-GA

To cover unmanned vessels and based on input from the above navigation sensors, a total system for determining the risk of collision and grounding and aiding in execution of a safe voyage plan should be provided. This system should use and process all available information from navigational sensors and systems in a robust manner in order to avoid single failures. In particular the following should be part of the system's capabilities:

- Collision avoidance function including anti-collision algorithms based on compliance with COLREG in all states of visibility
- Route monitoring function including anti-grounding algorithms coupled with the anti-collision algorithms
- Use of approved Electronic Navigational Charts (ENC) as basis for the world model
- Able to process all targets that may lead to a collision situation
- Operate in real-time
- Plan and evaluate updated voyage plan before execution
- Definition of the operational design domain and the ability to detect when outside this domain
- Alert management being compliant with the performance standards for Integrated Navigation Systems (INS) - ref. IMO Res. MSC.252(83) and subsequent the IMO bridge alert management (BAM) concept.

# APPENDIX E SIMULATOR BASED TESTING

## 1 General

Simulator based testing should provide objective evidence of suitable functionality (during normal, abnormal and degraded condition) of the specified target control system according to requirements defined in the specifications and in the relevant rules.

## 2 Test setup

Simulator based testing should be executed on the actual control system hardware to be installed on the vessel or on a replica control system, subject to Society's approval.

The simulator should run on a unit separate from the control system.

Testing should be performed on released software revisions for both simulator and control system(s) such that the software is uniquely identified.

Testing should be executed on the same test setup and software as validated through the test setup validation activity, and according to an approved test scope/program.

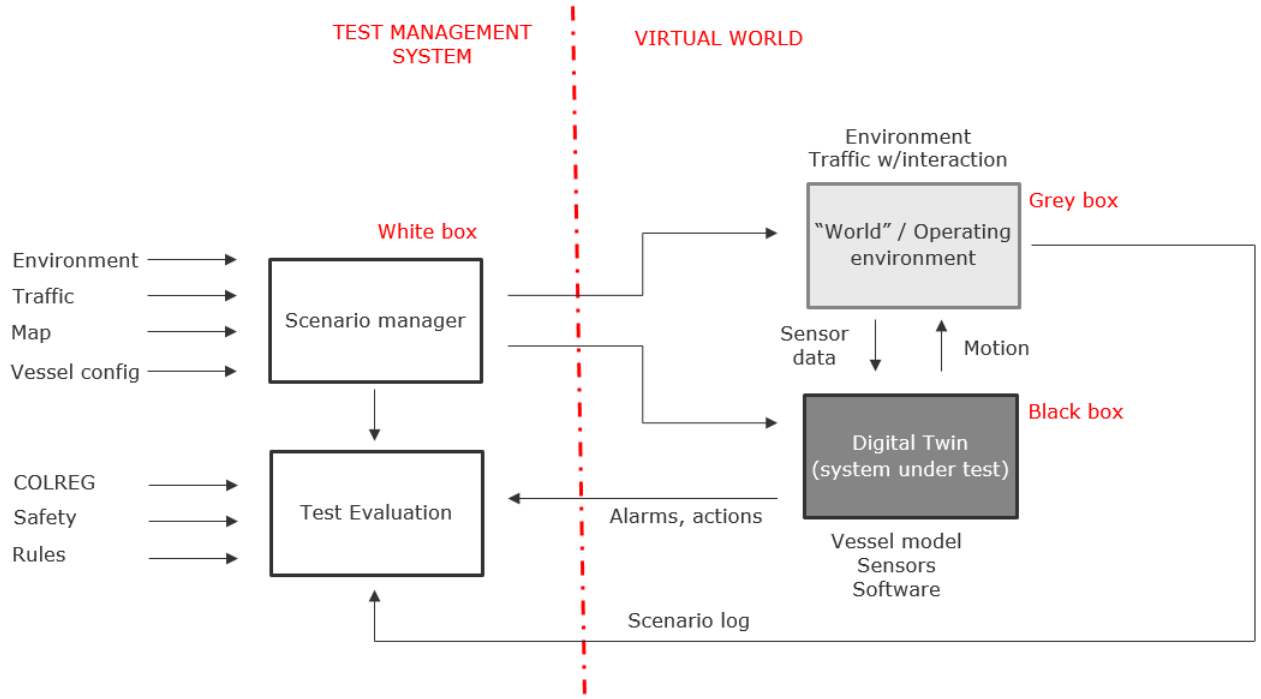


**Figure 1 Example of a simulator test setup for autoremote navigation functions**

## 3 Simulator framework

All (relevant) I/O should be interfaced between control system and simulator. If any signals are ignored/not interfaced, this should be documented and agreed upon in writing before test is executed.

It should be possible to monitor and/or trend all I/O-signals between simulator and control system.

It should be possible to introduce/simulate typical control system failures to the system, such as broken wire, value out of range, noise on signals, command errors (functions being executed without being commanded), execution errors (functions not being executed when commanded etc.).

The simulator should be adequate for the type of failures intended to be tested. Failures may either be introduced by manipulating the command or sensor signal, while others may have dynamic and/or spread effects, requiring to be generated from the simulator to propagate correctly to all affected signals.

## 4 Simulator accuracy and test setup validation

The simulator and control system should run in closed-loop and the simulator outputs should render a real-life behaviour of the system.

It should be possible to run all the functions in the control system (target system) without the need of manual manipulation of simulator signals. A simulator based test setup should be validated with validation tests demonstrating adequacy/suitability for the purpose (test objective) and that it does not mask errors in the target system. Before the validation testing is performed, it should be verified that there are no active nor ignored/suppressed alarms in the system that may have impact on the testing.

## 5 Simulator based test technologies

Known simulator based test methods are Hardware in the loop (HIL) and Software in the loop (SIL). The difference between these methods are if real hardware is used or emulated. Both methods are recognised methods for testing software, but SIL would normally simplify integration testing especially if different vendors are present provided that hardware emulators are available.

Simulators enables an extended scope for verification of the software as the possibility of failure modes and external forces, as environmental forces, may be added.

However, it is important to understand the limitation of simulator based testing as the hardware and IO layers are potentially left out of the test setup.

A complete test procedure should include all aspects of the control system setup according to requirements in DNVGL-RU-SHIP Pt.4 Ch.9 Sec.4.

## CHANGES – HISTORIC

There are currently no historical changes for this document.

**About DNV GL**

DNV GL is a global quality assurance and risk management company. Driven by our purpose of safeguarding life, property and the environment, we enable our customers to advance the safety and sustainability of their business. We provide classification, technical assurance, software and independent expert advisory services to the maritime, oil & gas, power and renewables industries. We also provide certification, supply chain and data management services to customers across a wide range of industries. Operating in more than 100 countries, our experts are dedicated to helping customers make the world safer, smarter and greener.

SAFER, SMARTER, GREENER