# Safety Critical Equipment and Spare Parts Guidance

(First edition 2018)

Issued by the

**Oil Companies International Marine Forum**
29 Queen Anne's Gate
London SW1H 9BU
England
Telephone: +44 (0)20 7654 1200
Fax: +44 (0)20 7654 1205

Email enquiries@ocimf.org

**www.ocimf.org**

**First edition 2018**


**The Oil Companies International Marine Forum (OCIMF)**
is a voluntary association of oil companies having an interest in the shipment and terminalling of crude oil and oil products. OCIMF is organised to represent its membership before, and consult with, the International Maritime Organization (IMO) and other government bodies on matters relating to the shipment and terminalling of crude oil and oil products, including marine pollution and safety.

**Terms of Use**
While the advice given in this information paper ("Paper") has been developed using the best information currently available, it is intended purely as guidance to be used at the user's own risk. No responsibility is accepted by the Oil Companies International Marine Forum ("OCIMF"), the membership of OCIMF or by any person, firm, corporation or organisation (who or which has been in any way concerned with the furnishing of information or data, the compilation or any translation, publishing or supply of the Paper) for the accuracy of any information or advice given in the Paper or any omission from the Paper or for any consequence whatsoever resulting directly or indirectly from compliance with, or adoption of or reliance on guidance contained in the Paper even if caused by a failure to exercise reasonable care.

## Contents

## Glossary

The following are agreed definitions for terms used within this paper.

**Catastrophic failure** Failure of a large piece of equipment where a large component fails which cannot be easily repaired or repaired at all on-site (such as engine crankshaft), or widespread damage to surrounding infrastructure (e.g. due to fire).

**Company** The owner of the ship, or any other organisation such as a ship manager or bareboat charterer that has assumed responsibility for the operation of the ship from the owner of the ship, including the duties and responsibilities imposed by the International Safety Management (ISM) Code. May also be referred to as operator.

**Degraded status** Operation of a vessel at a lower capacity after loss or partial loss of certain design features.

**Guidance** Provision of advice or information by OCIMF.

**Hazard** Any event/object that could cause harm.

**Hazard Identification Study (HAZID)** A structured, team-based approach to identify hazards, their potential consequences, and requirements for risk reduction.

**Hazard and Operability Study (HAZOP)** A structured, team-based approach to investigate how a system or plant in operation deviates from the design intent and creates risk for personnel and equipment and results in operability issues.

**Hazardous situation** A situation that may directly cause an accident that causes harm to people or the environment.

**Planned Maintenance System (PMS)** The part(s) of the company's Safety Management System (SMS) that address inspection, maintenance and repair of the vessel.

**Risk** The exposure to a hazard.

**Risk management policy** Company statement on how risks will be managed.

**Risk management process** Company's procedures within the SMS that address risk management.

**Risk management strategy** Company's structured approach to risk management.

**Safety critical equipment** An individual piece of equipment, a control system or an individual protection device which in the event of a single point failure may:

- Result in a hazardous situation which could lead to an accident.

Or

- Directly cause an accident that results in harm to people or the environment.

**Safety Management System (SMS)** The company's documented quality management system which addresses the requirements of the IMO ISM Code.

**Single point failure** Any single component failure that could lead to a hazardous situation or an accident.

## Abbreviations

| | |
|---|---|
| ALARP | As Low As Reasonably Practicable |
| DGE | Diesel Generator Engine |
| ECS | Engine Control System |
| HAZID | Hazard Identification Study |
| HAZOP | Hazard and Operability Study |
| HFO | Heavy Fuel Oil |
| HSSE | Health, Safety, Security and the Environment |
| IACS | International Association of Classification Societies |
| ICS | International Chamber of Shipping |
| IG | Inert Gas |
| IMO | International Maritime Organization |
| ISF | International Shipping Federation |
| ISM Code | International Safety Management Code |
| LTI | Lost Time Incident |
| MGO | Marine Gas Oil |
| MTBF | Mean Time Between Failures |
| OCIMF | Oil Companies International Marine Forum |
| OEM | Original Equipment Manufacturer |
| OVID | Offshore Vessel Inspection Database |
| PLC | Programmable Logic Controller |
| PMS | Planned Maintenance System |
| SIRE | Ship Inspection Report Programme |
| SMS | Safety Management System |
| SOLAS | International Convention for the Safety of Life at Sea |
| TMSA | Tanker Management and Self Assessment |
| VIQ | Vessel Inspection Questionnaire |

## Bibliography


### Oil Companies International Marine Forum (OCIMF)

*Tanker Management and Self Assessment (TMSA)*

SIRE Vessel Inspection Questionnaire (VIQ)

### International Maritime Organization (IMO)

*International Safety Management (ISM) Code*, Section 10.3

### International Shipping Federation (ISF) and the International Chamber of Shipping (ICS)

*Guidelines on the Application of the IMO International Safety Management (ISM) Code*

### Lloyd's Practical Shipping Guides

*The ISM Code: A Practical Guide to the Legal and Insurance Implications*

# 1 Introduction

The purpose of this information paper is to provide guidance on safety critical spare parts for companies to consider when preparing a Safety Management System (SMS). It is equally applicable to companies managing any type of vessel.

This paper introduces some boundary conditions to consider and walks through several steps that may be required to identify safety critical spare parts.

# 2 Key industry requirements and practices

This section explores current industry regulations, how they deal with safety critical spare parts and highlights the need for clarity.

The SMS that is developed and used by a company must fulfil the requirements defined at the highest level by the International Maritime Organization's (IMO) International Safety Management (ISM) Code. Section 1.2.2 of the International Safety Management Code (ISM Code) states that the safety management objectives of the company must assess all identified risks to its vessels, personnel and the environment and establish appropriate safeguards. The identification of safety critical equipment and use of safety critical spare parts can be considered as one of those safeguards. Section 8 of the ISM Code continues to outline requirements for emergency preparedness.

Section 10.3 of the ISM Code requires that mitigations are put in place within the company's SMS to avoid and manage hazardous situations. The question of what constitutes safety critical equipment is then addressed by section 10.3 of the ISM Code. Although this does not specifically state the terms 'critical' or 'safety critical', the industry generally accepts 'safety critical' as the term used to describe such equipment. Section 10.3 also introduces the concept of hazardous situations but does not continue to define what they may be.

OCIMF addresses risk management and hazard definition in Element 9 of *TMSA* and *Offshore Vessel Management and Self Assessment (OVMSA)*. The company should have a risk assessment programme that is designed to identify potential hazards and exposures and manage operational risks relating to HSSE.

The role of Classification Societies on spare parts has changed in recent years. Previous Class requirements for specific spares, based on International Association of Classification Societies (IACS) recommendations, have been replaced by guidance. It is important to note that the Class guidelines are generic and may not cover all the risks that a company must manage.

The ISM auditors, *TMSA*/*OVMSA* reviewer and SIRE inspectors play a key role in ensuring that companies apply the appropriate procedures, but it is generally difficult for an auditor to assess if a company considers safety critical equipment at the right level of detail. What they can assess is the company's consistent application of appropriate procedures in line with *TMSA*/*OVMSA* and VIQ/Offshore Vessel Inspection Database (OVID).

Simply following existing industry codes and practices may not address all risks. Legal challenges could be raised, following an incident, about whether the company has applied an appropriate level of due diligence when developing the company's risk management strategy. Companies may wish to seek legal advice on this matter, which can be fed into their strategy for maintaining safety critical equipment and application of safety critical spare parts.

# 3 The intent of safety critical spare parts

This section proposes some definitions and boundary limits to consider when evaluating the need for, and effectiveness of, safety critical spare parts.

## 3.1 Single point failures

A single point failure is any single component failure that could lead to a hazardous situation or an accident. The risk of single point failures exists because of generally predictable acts or events such as the inherent vessel design, incorrect installation, lack of planned maintenance or mis-operation. They may also occur due to unpredictable failures resulting from inherent manufacturing defects. For example, a loss of propulsion may occur as a result of a mechanical failure, electrical failure, explosion, fire or flood.

It may cause immediate harm or put the vessel at risk of experiencing a major accident such as a grounding, collision or allision.

Before a vessel operator can start to identify safety critical equipment and assess the need for the carriage of safety critical spare parts, they need to understand and document which single point failures may occur. This allows the criticality of each failure to be assessed at a later stage during the risk assessment process. The company should consider all systems, sub-systems, equipment and components which, in the event of a single point failure, could lead to the hazardous situation being realised and/or escalated.

Many of the high-level decisions on risk management are made for companies by industry trends and industry regulations (e.g. single main engines, redundancy in fire pumps or power generation). Therefore, an industry-standard vessel design could be used as the basis for a single point failure analysis in most cases.

A suggested starting point is to refer to system single line diagrams as the basis for identifying single point failures.

The evaluation could be tabulated using a logic flowchart to identify the potential outcome of each single point failure. The operator may develop a bespoke flowchart and worksheet to meet the needs of their business and incorporate it into their SMS. Simplified examples are provided in appendix A and appendix B.

## 3.2 Safety critical equipment

Safety critical equipment is an individual piece of equipment, a control system or an individual protection device which in the event of a single point failure may:

- Result in a hazardous situation which could lead to an accident.

Or

- Directly cause an accident that results in harm to people or the environment.

At the highest level, the company may consider loss of key vessel safety critical functions, which may include (but are not limited to) the following:

- Propulsion.
- Steering.
- Dead-ship recovery.
- Bilge management.
- Power generation and distribution.
- Power management.
- Automatic, integrated control and monitoring.
- Gas detection, oil mist detection, temperature monitoring.
- Communication.
- Key emergency response capability (including shut-down and fire-fighting).
- Life-saving appliances.
- Onboard loading computer (and damaged stability computer where applicable).
- Cargo management (safety systems and for emergency response).
- Inert Gas (IG).
- Ballast management (for emergency response).

Further levels of detail should be considered where it is clear that the diagram for the system under consideration does not provide sufficient detail for the company to make an appropriate decision. The company will need to decide what further level of detail is required in the Hazard Identification (HAZID) and Hazard and Operability (HAZOP) study process to meet their risk management policy: for example, from main engine(s) down to 12V control systems.

## 3.3 Safety critical spare parts

Safety critical spare parts are the spare components associated with the maintenance and repair of safety critical equipment.

## 3.4 Practical application of safety critical spare parts

To manage the risks associated with safety critical equipment, the inspection, testing and maintenance procedures for such equipment should be prioritised over all other maintenance. The procedures often include the use of safety critical spare parts, but they may also include materials and consumables required to execute a repair.

As unplanned maintenance may occur in deep sea with no other means of timely assistance available, it is recommended that an appropriate inventory of safety critical spare parts is carried on board the vessel at all times. However, it is recognised that there are limitations to the usefulness of safety critical spare parts in case of catastrophic failure events.

Safety critical spares which are carried on board can be used in two ways:

1. Proactively: Used on board during planned maintenance to ensure the reliability of the safety critical equipment to mitigate the occurrence of hazardous situations.
2. Reactively: Used on board during unplanned maintenance to repair damaged safety critical equipment to prevent a hazardous situation from escalating to a more serious uncontrolled incident.

In general, application of safety critical spare parts should help the ship's personnel to:

- Avoid premature failure of safety critical equipment by carrying out planned maintenance.

And

- Recover from the Safety of Life at Sea (SOLAS) dead-ship condition.
- Prevent a hazardous situation from escalating.
- Allow the vessel wherever possible, to reach a safe haven so that permanent repairs can be carried out.

There are cases when it may not be reasonable to expect the crew to be able to achieve the goals above by employing safety critical spare parts. For example:

- After catastrophic failure events where large pieces of equipment are damaged beyond repair (e.g. high energy failures that result in explosions, fires and flooding).
- After catastrophic failure events where extensive damage occurs to the vessel infrastructure.
- During heavy weather or due to other conditions where it is not possible to effect a timely repair (this should not be assumed to be the base case for the safety critical spare parts policy).

The company may find it useful to document a safety critical spare parts strategy, outlining the intent and limitations of their application. This may be generic for a fleet with specific requirements for a Class of vessels or one on a particularly sensitive trade.

A key concept to consider is that the ship's personnel should be able to deploy safety critical spare parts in a timely manner to manage the immediate risks. The company should consider defining what they understand to be a timely manner (appropriate for the type of vessels they operate and the vessel trade routes) as part of the risk management process.

For most large components (e.g. engine crankshaft, propeller, etc.) it is recognised that the company may not consider it reasonable for the vessel to carry and employ spares. However, such decisions should be justified through the risk assessment and management process.

# 4 Safety critical spare parts and safety management systems

This section discusses where safety critical systems and safety critical spare parts may be addressed in a company SMS.

It is recommended that a proactive risk-based approach to the carriage of safety critical spare parts is taken for the management of hazardous situations. This approach may need to be above and beyond minimum regulatory requirements. Companies should apply this approach to both new-builds and to existing vessels.

The key elements of an SMS that facilitate the identification and implementation of safety critical equipment and safety critical spare parts are:

1. HSSE management policy and framework.
2. Risk management strategy.
3. Documented hazard identification process.
4. Documented process which defines the manager's heirarchy of HSSE Controls.
5. Documented risk assessment and ranking process.
6. Documented process to tie risk mitigations to each risk, including use of safety critical spare parts.
7. Documented policy which states the requirements for, and carriage of safety critical spare parts.
8. Procedures to manage the procurement, carriage, use and onboard inventory of safety critical spare parts.

Additionally, safety critical equipment and safety critical spare parts should be addressed in the company management of change process should a vessel's trade change significantly and results in new risks and/or higher consequences. The process should also be employed when new/existing tonnage is introduced into the owner's fleet.

Although it is not necessary to consider business continuity when considering safety critical equipment and safety critical spare parts, companies could find it helpful to think about what constitutes business critical equipment and business critical spare parts.

Business critical equipment and business critical spare parts refers to the equipment and spare parts carried to ensure vessel reliability from a business delivery perspective, in addition to safety critical equipment and safety critical spare parts, e.g. cargo pumps. This activity may help justify and draw a clear line between what is strictly a safety critical item and what is a business critical item.

The process for considering business critical equipment and business critical spare parts may be common with the process of defining safety critical equipment and safety critical spare parts. In the case of business critical equipment failure, the risks would be recorded as business risks, rather than HSSE risks.

The following sub-sections support the consideration of safety critical spare parts in an SMS.

## 4.1 Risk management strategy

In general, and in the first instance, hazardous situations are avoided by appropriate vessel design and equipment, and the application of safe working practices, such as those required by SOLAS and the ISM Code. For example:

- By installing redundant or alternate equipment and systems with appropriate system segregation (multiple safety critical equipment).

This considers that any equipment can suffer a failure and addresses the situation where the failure, as determined by the company risk assessment, cannot be tolerated.

- A reliability-centred approach, employing high reliability equipment (safety critical equipment such as single main engine).

Failure can be tolerated, perhaps only for a limited period of time, where certain safety critical spare parts can reasonably be employed in a timely manner (e.g. main engine/main engine piston).

- The employment of a proactive planned maintenance system (employing safety critical spare parts).
- The development of safe operating procedures as an alternative or back-up to design controls.

The escalation of hazardous situations is then prevented or managed by employing alternate operating procedures to allow the vessel to be stabilised to continue on passage or sail to a safe port of refuge. This includes:

- Onboard unplanned maintenance capabilities (employing safety critical spare parts).
- Vessel emergency response systems (proactively maintained as safety critical equipment).
- Employing alternative working practices (including operation with degraded capability).
- Access to third-party intervention wherever possible (such as an emergency towing service).

It could be argued that the stand-by unit in a set of redundant equipment is not safety critical equipment. However, if the primary unit fails and the intention is for the stand-by unit to operate with immediate effect to mitigate the hazard(s), the company may deem that the stand-by unit also needs to be inspected, tested, maintained and repaired as a piece of safety critical equipment.

There is also the issue of segregation to consider if all equipment and auxiliaries are in one space. If that space suffers from a major fire, explosion or flood, equipment redundancy in that space is ineffective and safety critical spare parts may not be effective to reactively manage the incident. For fully segregated systems, safety critical spare parts remain a key part of the planned maintenance process. The segregation of redundant units suggests a particularly high criticality on immediate availability.

Once the risk assessment process is complete, the operator should select appropriate risk reduction measures (i.e. HSSE controls, equipment redundancy, safety critical spare parts) and implement them to manage risks to an appropriate level (e.g. As Low as Reasonably Practicable (ALARP) or another pre-defined key performance indicator). The final output from the hazard identification and risk assessment process should demonstrate that each risk has been controlled. Resulting design mitigations should be considered and added to the vessel specification, or procedural mitigations incorporated into the SMS where it is not possible or reasonable to add a design mitigation.

## 4.2 ALARP and the Hierarchy of HSSE Controls

The understanding of the term ALARP and the application of the Hierarchy of HSSE Controls varies across the industry. Therefore, the following clarifications are suggested for consideration.

**ALARP**

The term ALARP originates from the United Kingdom Health and Safety at Work act. The term ALARP is commonly mentioned in shipping but the practical definition can be subjective and can vary from company to company. Therefore, the company should endeavour to clearly define what it means to them based on the prevailing regulatory and legal environment, insurance implications, contractual obligations and the company policy on risk management.

**Hierarchy of HSSE Controls**

The hierarchy of HSSE controls could also be defined within the operator's HSSE management framework and applied in the process of managing identified risks. The following hierarchy, in descending order of effectiveness, is provided as guidance only, but is widely accepted across many industries:

1. Elimination: Avoid exposure to the potential hazard in the first instance to eliminate the risk.
2. Substitution: Substitute the working method with an alternative process or way of working.
3. Engineering controls: The implementation of physical changes to the vessel which eliminates or reduces the hazard. This is achieved through proactive vessel design or reactive modification and includes redundancy and segregation of equipment, systems and personnel where appropriate. These are defined at an industry level by IMO conventions, state regulations or by other industry bodies. They may also be supplemented when found necessary by the company to address a particular risk.
4. Administrative and work practice controls: Establish processes or procedures to mitigate or manage the hazards (SMS procedures). These are also required or implied by regulations and industry guidelines.

Administrative controls may also be applied as back-up, or temporary controls when engineering controls are rendered inoperable or prove to be inadequate. Temporary controls may allow the vessel to continue normal operations but they may result in the vessel operating with a degraded capability. This may allow a damaged vessel to reach a safe port of refuge to make permanent repairs.

## 4.3 General considerations for hazard identification and risk assessments

The identification of safety critical equipment and establishing the need for safety critical spare parts can only take place after a methodical hazard identification has been carried out. A multi-disciplinary team should be brought together to carry out this work (e.g. including engineers, naval architects, electrical specialists, vessel superintendents).

The hazard identification and risk assessment process should strive to answer the following questions:

- What are the sources of stored energy?
- Which hazardous situations may occur on the vessel and trade under consideration?
- What could cause the situation to occur?
- What could cause the situation to escalate?
- What is the likelihood of the situation occurring?
- What are the potential consequences when a hazardous situation is not controlled?
- Are the consequences tolerable in all operational scenarios?
- If not, how can the situations be prevented from occurring?
- If they cannot be prevented, how can they be managed?

The hazard identification and risk assessment process should also consider:

- The vessel type.
- The vessel operating profile/trade route for each type of vessel.
- Operational procedures.
- The inherent vessel design (system redundancy and segregation).
- Original Equipment Manufacturer's (OEM) advice, industry experience, fleet experience of equipment Mean Time Between Failures (MTBF).
- New technologies applied.

High-potential situations which could cause harm to many people and extensive damage to the environment should be specifically highlighted as part of this process. For example, risks related to navigation, hydrocarbon handling systems, or any other high-potential risks as determined by the owner.

The risk assessment will be common in many areas for all vessel types in the operator's fleet, but additional risks may be identified for specific vessel types, cargoes and trades. As a minimum, the risk assessment and management documentation should indicate:

- How frequently each hazardous situation could occur.
- The consequences of their occurrence.
- Whether the systems under consideration are, consequently, to be deemed safety critical.
- How failures are to be mitigated for each identified risk.
- Where safety critical spare parts could reasonably be used reactively as a mitigating action.
- What residual risks remain after HSSE controls have been applied.

Establishing the likelihood of a hazardous situation or accident occurring can be a significant challenge. In many cases the operator does not have direct knowledge or sufficient experience of certain types of incidents (and as a result, data collected) to be able to make informed judgements. Frequency data (i.e. MBTF) is not always widely published within the industry. In addition, for new vessel trades or technologies, this data is also not generally available. Therefore, the company should take a pragmatic view when assessing likelihood of an event occurring, and could consider in the following order:

- Which events have occurred within the company's fleet and their frequency (available information).
- Which events have occurred within the industry and the frequency of their occurrence (where information is available).
- Which events are possible, despite lack of documented industry experience.

In the third point above, the company may choose to identify certain high-impact events which they deem possible. As the events are considered possible and high-impact, they would need to be mitigated with particularly robust HSSE controls. An example could be generator engines redundancy.

The results obtained for each consequence identified by the risk assessment may be plotted on a risk-ranking matrix to illustrate compliance with the company's criteria for risk management. The risk assessment should be updated on a periodic basis and additionally if there are any changes to the company's operations, the company's experience, the OEM's service experience (where available) or when new vessels are brought into the fleet.

It would be helpful for the company's HSSE management framework to include a high-level definition that categorises the consequences of an accident occurring. This can help the manager decide on appropriate risk mitigations. For example, HSSE consequences of safety critical equipment failure may include:

- Harm to people on board.
- Harm to other people.
- Harm to the environment.

The framework should identify several impact levels for each category of consequence. As an example, for harm to people the consequences may include first-aid cases, Lost Time Incidents (LTI), fatality and multiple fatalities. This allows the vessel operator to establish a criticality for each risk mitigation.

# 5 Planned maintenance systems

## 5.1 General considerations for planned maintenance systems

This section proposes several considerations for addressing safety critical spare parts in the Planned Maintenance System (PMS).

Specific provisions must be included in the PMS to enable and help ship's personnel carry out safety critical equipment maintenance. However, it should be remembered that if ship's personnel are physically unable to carry out a maintenance task on safety critical equipment, the parts themselves are not going to be effective to prevent or manage an incident. This is particularly relevant for high-risk, unplanned maintenance on safety critical equipment.

A PMS that recognises the importance of maintenance on safety critical equipment or systems would address the following list of key items:

- Procedures which specifically address safety critical equipment and systems and the use of safety critical spare parts.
- Inspection, maintenance and testing of safety critical equipment and systems is prioritised over all other maintenance.
- Inspection, maintenance and testing of safety critical equipment and systems is carried out according to specified mandatory requirements.
- Safety critical equipment and systems is clearly identified in the PMS and in maintenance task lists.
- A requirement to maintain a minimum inventory of safety critical spare parts, consumables and materials.
- Procedures that define minimum personnel competency and experience requirements for each task.
- Guidance for the use of specialist or OEM support (including remote diagnostics where applicable).
- Instructions for ship's personnel on how to carry out safety critical equipment maintenance tasks.
- Risk assessments are required for all maintenance tasks on safety critical equipment.
- Guidance for ship's personnel on acceptable temporary repairs.
- A requirement that ensures the correct tools, manuals and drawings to maintain safety critical equipment are available on board.
- Deferment of planned maintenance for safety critical equipment is only approved by shore personnel for a finite period with any repeated requests for deferment being escalated to an appropriate higher level of shore management.
- Deferment of safety critical equipment planned maintenance is based on a documented risk-assessment which is recorded, time limited and may require additional HSSE controls imposed to mitigate the risk.
- Safety critical equipment failures should be investigated by discipline subject matter experts and the maker.
- Safety critical equipment failures are highlighted in the incident reporting system for high visibility to management.

## 5.2 Procedures

The management of safety critical spare parts on board a vessel needs to be carefully controlled to ensure that the spares are ready for use at any time. This includes inventory management, enabling materials and procurement controls which prioritise the replacement of consumed safety critical spare parts.

Generic procedures may be included in the PMS for common safety critical equipment maintenance tasks for the owner's fleet, supplemented by procedures specific to each vessel type/Class and operating environment where required.

Permanent or temporary alternate HSSE controls for degraded status operations should be documented in the procedures, where appropriate. These are required to manage potentially hazardous situations during maintenance of safety critical equipment, if the safety critical equipment does not have redundancy or ultimately cannot be repaired. The identification of alternate controls should be addressed in the risk assessment process.

## 5.3 Enabling materials

The vessel should have any materials required to deploy the safety critical spare parts, including tools, drawings, manuals and materials, readily available at all times.

The term spare parts is usually understood to mean the physical parts of a piece of equipment (or system). However, spare and perishable materials (such as lube oils, plates, pipes, clamps, nuts, bolts, fillers, welding consumables, gasket materials) may also need to be available and may be essential to enable the use of safety critical spare parts in the event of a material failure or the return to service of the equipment being maintained. The company should ensure that an appropriate inventory of such items is also maintained on board at all times, as far as reasonably practicable. However, it is understood that if safety critical spare parts are used for unplanned maintenance at sea, there may be some periods when those spares are not carried on board while replacements are procured.

Temporary repair materials should not be carried with the intention of making repairs instead of employing appropriate safety critical spare parts, when the parts are readily available or instead of systems redundancy.

It is also important to recognise that temporary repairs to safety critical systems may require degraded status operational controls to be put in place. Temporary repairs should be replaced by permanent repairs as soon as it is reasonably safe to do so.

## 5.4 Procurement and quality control

The company follows a clearly defined policy for the procurement of safety critical spare parts to ensure that appropriate, safety critical spare parts of a verifiable quality are procured. The policy clearly states requirements for the use of OEM safety critical spare parts, OEM-licensed spare parts and after-market spare parts.

The need for and procurement of safety critical spare parts should be addressed in all new-build spares inventories.

## 5.5 Inventory management

Procedures should ensure that the shelf-life of components is addressed. The operator should proactively, and as far as reasonably practicable, make every effort to ensure that the inventory of ready-to-deploy safety critical spare parts does not drop below the minimum-specified quantities at any time. Electronic components such as programmable logic controllers (PLCs) should have firmware updates where recommended by the manufacturer on a periodic basis to ensure that they are ready for service at any time. It is recommended that the component supplier presents to the owner an agreed plan on how requirements for software updates are communicated to the company and subsequently executed on board. Records of firmware updates should be maintained.

Procedures should also address the preservation, periodic inspection and stock-checking of the safety critical spare parts inventory. This should include the potential obsolescence of spares.

The company should carefully consider the implications of lead time in their inventory management procedures, particularly when safety critical spare parts are used for unplanned maintenance. Some long lead time spares may need to be held centrally in a fleet store where despatch to vessels can be made promptly.

## 5.6 Identification of safety critical spare parts in the planned maintenance system

The identification of safety critical equipment should be in an easy-to-understand format. A summary of all safety critical equipment should be available in a list or matrix format. In a computerised PMS, safety critical equipment should be provided with computer-searchable tags. Information provided in the PMS could be as follows:

- Safety critical equipment reference number.
- Description of the safety critical equipment.
- Explanation of its function in the risk management strategy.
- Information on the principal equipment and components.
- References to procedures and special instructions.

## 5.7 Vendor support

As modern vessels increasingly rely upon automation, many systems are operated by proprietary control systems which the ship's personnel cannot interrogate or repair. The need for remote diagnosis and repair of electronic systems is increasing. A vendor support/emergency response contract may be needed as part of the safety critical equipment planned and unplanned maintenance strategy. Consideration should be given to the company's cyber risk management procedures which may restrict or prevent ship-to-vendor connectivity.

Remote support should only be a back-up to appropriate vessel design and operational procedures, including the use of physical spares. Remote assistance may not always be available for technical reasons. This does highlight the importance of the reliability of the broadband communication systems on vessels where remote support may be of benefit and part of the operational strategy.

# 6 Conclusions

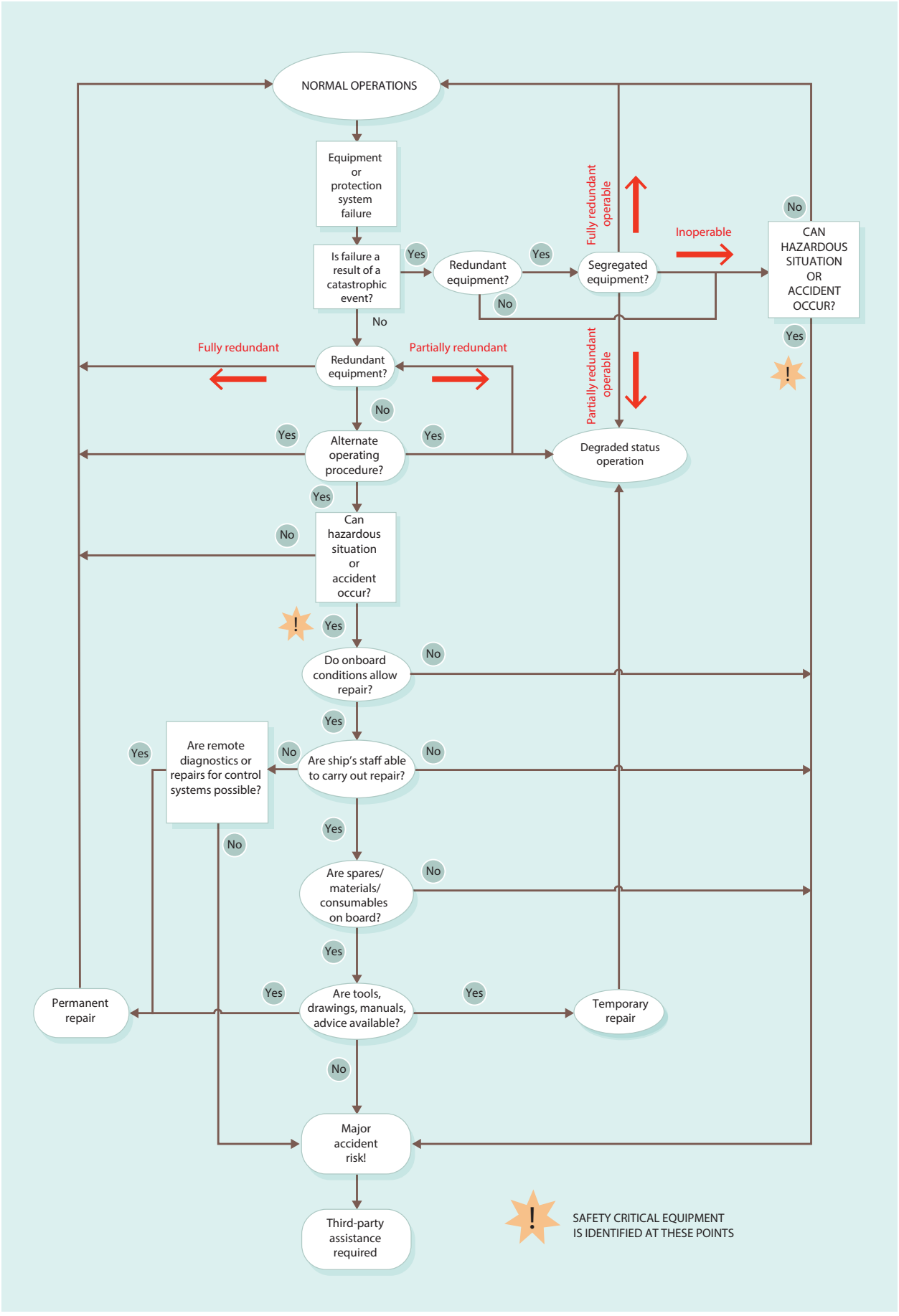
The identification of safety critical equipment and the need for safety critical spare parts is a complicated subject and there is no one-size-fits-all solution. It can be a contentious subject and stakeholder views can be subjective.

Companies should take comfort that the framework for developing a robust SMS already exists in the marine industry. This paper provides guidance on the challenges that may be encountered when considering safety critical spare parts so that the owner can strive to efficiently manage their risks. The paper will encourage further discussion within the industry and within a company's technical management organisation.

# Appendix A Considerations for identification of hazardous situations

| Hazardous situation | Potential accident | Consequences | Associated system failure (main and auxiliary) | Mitigation/system redundancy | Alternate process |
|---|---|---|---|---|---|
| Loss of power | Collision, allision, grounding, explosion, fire and flood | Harm to the environment<br>Harm to people | Generator engines<br>Generators<br>Switchboards<br>Fuel supply system<br>Power management system<br>Engine Control System (ECS) | Multiple Diesel Generator Engines (DGEs), emergency DGE<br>Multiple gensets, emergency genset<br>Split switchboards<br>Yes – multiple systems<br>Yes – full redundancy<br>Yes – full redundancy | Use fully redundant DGE<br>Use fully redundant DGE<br>Degraded operation<br>Heavy Fuel Oil (HFO) and Marine Gas Oil (MGO) fuel systems<br>Use redundant power management system<br>Use redundant ECS |
| Loss of propulsion | Collision, allision, grounding, explosion, fire and flood | Harm to the environment<br>Harm to people | Main propulsion system<br>Fuel supply system<br>Power management system<br>ECS<br>Start air system<br>Stern tube cooling/lubrication<br>Etc. | Single point failure<br>Yes – multiple systems<br>Yes – full redundancy<br>Yes – full redundancy<br>Partial system redundancy<br>Single point failure | Third-party intervention<br>Spares/use alternative fuel systems<br>Spares/remote diagnostics<br>Spares/manual, local control<br>Spares<br>Spares/third-party intervention |
| Loss of steering | Collision, allision, grounding, explosion, fire and flood | Harm to the environment<br>Harm to people | Steering gear<br>Hydraulic system<br>Helm/autopilot<br>Etc. | Single point failure<br>Yes – redundant pumps<br>Yes – redundant control | Third-party intervention<br>Spare hydraulic pumps<br>Local manual control |
| Loss of Inert Gas (IG) system | Explosion | Harm to the environment<br>Harm to people | Fuel supply system<br>IG generator (boiler)<br>IG supply system<br>IG control system<br>Etc. | Partial redundancy<br>Partial redundancy (boilers)<br>Partial redundancy<br>Single point failure | Yes<br>Degraded capacity (IG generator)<br>None<br>Spares/remote diagnostics |
| Loss of gas monitoring system | Explosion<br>Suffocation | Harm to the environment<br>Harm to people | Fixed gas monitoring and alarm system<br>Etc. | Partial redundancy | Spares/portable gas monitoring |
| Failure of cargo/ballasting monitoring equipment | Loss of containment | Harm to the environment<br>Harm to people | Level alarms<br>Gas detectors | Safety policies<br>Safety policies | Manual observations<br>Manual observations |
| Loss of mooring | Collision, allision | Harm to the environment<br>Harm to people<br>Harm to infrastructure | Mooring winches<br>Mooring lines | Equipment redundancy | Spares<br>Spares |

# Appendix B Example flowchart for the identification of safety critical systems and spare parts




A voice for safety

**Oil Companies**
**International Marine Forum**
29 Queen Anne's Gate
London SW1H 9BU
United Kingdom

**T** +44 (0)20 7654 1200
**F** +44 (0)20 7654 1205
**E** enquiries@ocimf.org
**ocimf.org**