Guide for Failure Mode and Effect Analysis

Effective from 1 January 2017

Emirates Classification Society (Tasneef)
Aldar HQ 19th Floor,
Al Raha Beach, Abu Dhabi, UAE
Abu Dhabi, United Arab Emirates

Phone (+971) 2 692 2333
Fax (+971) 2 445 433
P.O. Box. 111155
info@tasneef.ae

GENERAL CONDITIONS

Definitions:

"*Administration*" means the Government of the State whose flag the Ship is entitled to fly or under whose authority the Ship is authorised to operate in the specific case.

"IACS" means the International Association of Classification Societies.

"*Interested Party*" means the party, other than the Society, having an interest in or responsibility for the Ship, product, plant or system subject to classification or certification (such as the owner of the Ship and his representatives, the ship builder, the engine builder or the supplier of parts to be tested) who requests the Services or on whose behalf the Services are requested.

"*Owner*" means the registered owner, the ship owner, the manager or any other party with the responsibility, legally or contractually, to keep the ship seaworthy or in service, having particular regard to the provisions relating to the maintenance of class laid down in Part A, Chapter 2 of the Rules for the Classification of Ships or in the corresponding rules indicated in the specific Rules.

"Rules" in these General Conditions means the documents below issued by the Society:

(i) Rules for the Classification of Ships or other special units;
(ii) Complementary Rules containing the requirements for product, plant, system and other certification or containing the requirements for the assignment of additional class notations;
(iii) Rules for the application of statutory rules, containing the rules to perform the duties delegated by Administrations;
(iv) Guides to carry out particular activities connected with Services;
(v) Any other technical document, as for example rule variations or interpretations.

"*Services*" means the activities described in Article 1 below, rendered by the Society upon request made by or on behalf of the Interested Party.

"Ship" means ships, boats, craft and other special units, as for example offshore structures, floating units and underwater craft.

"*Society*" or *"TASNEEF"* means Tasneef and/or all the companies in the Tasneef Group which provide the Services.

"*Surveyor*" means technical staff acting on behalf of the Society in performing the Services.

Article 1

1.1. The purpose of the Society is, among others, the classification and certification of ships and the certification of their parts and components. In particular, the Society:
(i) sets forth and develops Rules;
(ii) publishes the Register of Ships;
(iii) issues certificates, statements and reports based on its survey activities.

1.2. The Society also takes part in the implementation of national and international rules and standards as delegated by various G overnments.

1.3. The Society carries out technical assistance activities on request and provides special services outside the scope of classification, which are regulated by these general conditions, unless expressly excluded in the particular contract.

Article 2

2.1. The Rules developed by the Society reflect the level of its technical knowledge at the time they are published. Therefore, the Society, although committed also through its research and development services to continuous updating of the Rules, does not guarantee the Rules meet state-of-the-art science and technology at the time of publication or that they meet the Society's or others' subsequent technical developments.

2.2. The Interested Party is required to know the Rules on the basis of which the Services are provided. With particular reference to Classification Services, special attention is to be given to the Rules concerning class suspension, withdrawal and reinstatemen t. In case of doubt or inaccuracy, the Interested Party is to promptly contact the Society for clarification.
The Rules for Classification of Ships are published on the Society's website: www.tasneef.ae.

2.3. The Society exercises due care and skill:
(i) in the selection of its Surveyors
(ii) in the performance of its Services, taking into account the level of its technical knowledge at the time the Services are performed.

2.4. Surveys conducted by the Society include, but are not limited to, visual inspection and non-destructive testing. Unless otherwise required, surveys are conducted through sampling techniques and do not consist of comprehensive verification or monitoring of the Ship or of the items subject to certification. The surveys and checks made by the Society on board ship do not necessarily require the constant and continuous presence of the Surveyor. The Society may also commission laboratory testing, underwater inspection and other checks carried out by and under the responsibility of qualified service suppliers. Survey practices and procedures are selected by the Society based on its experience and knowledge and according to generally accepted technical standards in the sector.

Article 3

3.1. The class assigned to a Ship, like the reports, statements, certificates or any other document or information issued by the Society, reflects the opinion of the Society concerning compliance, at the time the Service is provided, of the Ship or product subject to certification, with the applicable Rules (given the intended use and within the relevant time frame).
The Society is under no obligation to make statements or provide information about elements or facts which are not part of th e specific scope of the Service requested by the Interested Party or on its behalf.

3.2. No report, statement, notation on a plan, review, Certificate of Classification, document or information issued or given as p art of the Services provided by the Society shall have any legal effect or implication other than a representation that, on the basis of the checks made by the Society, the Ship, structure, materials, equipment, machinery or any other item covered by such document or information meet the Rules. Any such document is issued solely for the use of the Society, its committees and clients or other duly authorised bodies and for no other purpose. Therefore, the Society cannot be held liable for any act made or document issued by other parties on the basis of the statements or information given by the Society. The validity, application, meaning and interpretation of a Certificate of Classification, or any other document or information issued by the Society in connection with its Services, is governed by the Rules of the Society, which is the sole subject entitled to make such interpretation. Any disagreement on technical matters between the Interested Party and the Surveyor in the carrying out of his functions shall be raised in writing as soon as possible with the Society, which will settle any divergence of opinion or dispute.

3.3. The classification of a Ship, or the issuance of a certificate or other document connected with classification or certificati on and in general with the performance of Services by the Society shall have the validity conferred upon it by the Rules of the Society at the time of the assignment of class or issuance of the certificate; in no case shall it amount to a statement or warranty of seaw orthiness,

structural integrity, quality or fitness for a particular purpose or service of any Ship, structur e, material, equipment or machinery inspected or tested by the Society.

3.4. Any document issued by the Society in relation to its activities reflects the condition of the Ship or the subject of certifi cation or other activity at the time of the check.

3.5. The Rules, surveys and activities performed by the Society, reports, certificates and other documents issued by the Society are in no way intended to replace the duties and responsibilities of other parties such as Governments, designers, ship builders, manufacturers, repairers, suppliers, contractors or sub-contractors, Owners, operators, charterers, underwriters, sellers or intended buyers of a Ship or other product or system surveyed.

These documents and activities do not relieve such parties from any fulfilment, warranty, responsibility, duty or obligation (also of a contractual nature) expressed or implied or in any case incumbent on them, nor do they confer on such parties any right, claim or cause of action against the Society. With particular regard to the duties of the ship Owner, the Services undertaken by the Society do not relieve the Owner of his duty to ensure proper maintenance of the Ship and ensure seaworthiness at all times. Likewise, t he Rules, surveys performed, reports, certificates and other documents issued by the Society are intended neither to guarantee the buyers of the Ship, its components or any other surveyed or certified item, nor to relieve the seller of the duties arising out of the law or the contract, regarding the quality, commercial value or characteristics of the item which is the subject of transaction.

In no case, therefore, shall the Society assume the obligations incumbent upon the above-mentioned parties, even when it is consulted in connection with matters not covered by its Rules or other documents.

In consideration of the above, the Interested Party undertakes to relieve and hold harmless the Society from any third party claim, as well as from any liability in relation to the latter concerning the Services rendered.

Insofar as they are not expressly provided for in these General Conditions, the duties and responsibilities of the Owner and Interested Parties with respect to the services rendered by the Society are described in the Rules applicable to the specific Service rendered.

Article 4

4.1. Any request for the Society's Services shall be submitted in writing and signed by or on behalf of the Interested Party. Such a request will be considered irrevocable as soon as received by the Society and shall entail acceptance by the applicant of all relevant requirements of the Rules, including these General Conditions. Upon acceptance of the written request by the Society, a contract between the Society and the Interested Party is entered into, which is regulated by the present General Conditions.

4.2. In consideration of the Services rendered by the Society, the Interested Party and the person requesting the service shall be jointly liable for the payment of the relevant fees, even if the service is not concluded for any cause not pertaining to the Society. In the latter case, the Society shall not be held liable for non-fulfilment or partial fulfilment of the Services requested. In the event of late payment, interest at the legal current rate increased by 1.5% may be demanded.

4.3. The contract for the classification of a Ship or for other Services may be terminated and any certificates revoked at the request of one of the parties, subject to at least 30 days' notice to be given in writing. Failure to pay, even in part, the fees due for Services carried out by the Society will entitle the Society to immediately terminate the contract and suspend the Services.

For every termination of the contract, the fees for the activities performed until the time of the termination shall be owed to the Society as well as the expenses incurred in view of activities already programmed; this is without prejudice to the right to compensation due to the Society as a consequence of the termination.

With particular reference to Ship classification and certification, unless decided otherwise by the Society, termination of the contract implies that the assignment of class to a Ship is withheld or, if already assigned, that it is suspended or withdrawn; any st atutory certificates issued by the Society will be withdrawn in those cases where provided for by agreements between the Society and the flag State.

Article 5

5.1. In providing the Services, as well as other correlated information or advice, the Society, its Surveyors, servants or agents operate with due diligence for the proper execution of the activity. However, considering the nature of the activities performed (see art. 2.4), it is not possible to guarantee absolute accuracy, correctness and completeness of any information or advice supplied. Express and implied warranties are specifically disclaimed.

Therefore, except as provided for in paragraph 5.2 below, and also in the case of activities carried out by delegation of Governments, neither the Society nor any of its Surveyors will be liable for any loss, damage or expense of whatever nature sustained by any person, in tort or in contract, derived from carrying out the Services.

5.2. Notwithstanding the provisions in paragraph 5.1 above, should any user of the Society's Services prove that he has suffered a loss or damage due to any negligent act or omission of the Society, its Surveyors, servants or agents, then the Society will pay compensation to such person for his proved loss, up to, but not exceeding, five times the amount of the fees charged for the specific services, information or opinions from which the loss or damage derives or, if no fee has been charged, a maximum of AED5,000 (Arab Emirates Dirhams Five Thousand only). Where the fees charged are related to a number of Services, the amount of the fees will be apportioned for the purpose of the calculation of the maximum compensation, by reference to the estimated time involved in the performance of the Service from which the damage or loss derives. Any liability for indirect or consequential loss, damage or expense is specifically excluded. In any case, irrespective of the amount of the fees charged, the maximum damages payable by the Society will not be more than AED5,000,000 (Arab Emirates Dirhams Five Millions only). Payment of compensation under this paragraph will not entail any admission of responsibility and/or liability by the Society and will be made without prejudice to the disclaimer clause contained in paragraph 5.1 above.

5.3. Any claim for loss or damage of whatever nature by virtue of the provisions set forth herein shall be made to the Society in writing, within the shorter of the following periods: (i) THREE (3) MONTHS from the date on which the Services were performed, or (ii) THREE (3) MONTHS from the date on which the damage was discovered. Failure to comply with the above deadline will constitute an absolute bar to the pursuit of such a claim against the Society.

Article 6

6.1. These General Conditions shall be governed by and construed in accordance with United Arab Emirates (UAE) law, and any dispute arising from or in connection with the Rules or with the Services of the Society, including any issues concerning responsibility, liability or limitations of liability of the Society, shall be determined in accordance with UAE law. The courts of the Dubai International Financial Centre (DIFC) shall have exclusive jurisdiction in relation to any claim or dispute which may arise out of or in connection with the Rules or with the Services of the Society.

6.2. However,

(i) In cases where neither the claim nor any counterclaim exceeds the sum of AED300,000 (Arab Emirates Dirhams Three Hundred Thousand) the dispute shall be referred to the jurisdiction of the DIFC Small Claims Tribunal; and

(ii) for disputes concerning non-payment of the fees and/or expenses due to the Society for services, the Society shall have the

right to submit any claim to the jurisdiction of the Courts of the place where the registered or operating office of the Interested Party or of the applicant who requested the Service is located.

In the case of actions taken against the Society by a third party before a public Court, the Society shall also have the right to summon the Interested Party or the subject who requested the Service before that Court, in order to be relieved and held harmless according to art. 3.5 above.

Article 7

7.1. All plans, specifications, documents and information provided by, issued by, or made known to the Society, in connection with the performance of its Services, will be treated as confidential and will not be made available to any other party other than the Owner without authorisation of the Interested Party, except as provided for or required by any applicable international, European or domestic legislation, Charter or other IACS resolutions, or order from a competent authority. Information about the status and validity of class and statutory certificates, including transfers, changes, suspensions, withdrawals of class, recommendations/conditions of class, operating conditions or restrictions issued against classed ships and other related information, as may be required, may be published on the website or released by other means, without the prior consent of the Interested Party.

Information about the status and validity of other certificates and statements may also be published on the website or released by other means, without the prior consent of the Interested Party.

7.2. Notwithstanding the general duty of confidentiality owed by the Society to its clients in clause 7.1 above, the Society's clients hereby accept that the Society may participate in the IACS Early Warning System which requires each Classification Society to provide other involved Classification Societies with relevant technical information on serious hull structural and engineering systems failures, as defined in the IACS Early Warning System (but not including any drawings relating to the ship which may be the specific property of another party), to enable such useful information to be shared and used to facilitate the proper working of the IACS Early Warning System. The Society will provide its clients with written details of such information sent to the involved Classification Societies.

7.3. In the event of transfer of class, addition of a second class or withdrawal from a double/dual class, the Interested Party undertakes to provide or to permit the Society to provide the other Classification Society with all building plans and drawings, certificates, documents and information relevant to the classed unit, including its history file, as the other Classification Society may require for the purpose of classification in compliance with the applicable legislation and relative IACS Procedure. It is the Owner's duty to ensure that, whenever required, the consent of the builder is obtained with regard to the provision of plans and drawings to the new Society, either by way of appropriate stipulation in the building contract or by other agreement.

In the event that the ownership of the ship, product or system subject to certification is transferred to a new subject, the latter shall have the right to access all pertinent drawings, specifications, documents or information issued by the Society or which has come to the knowledge of the Society while carrying out its Services, even if related to a period prior to transfer of ownership.

Article 8

8.1. Should any part of these General Conditions be declared invalid, this will not affect the validity of the remaining provisions.

INDEX

INDEX

1 GENERAL

1.1 Introduction

1.1.1 FMEA purpose

A practical, realistic and documented assessment of the failure characteristics of a complex system should be undertaken with the aim of defining and studying its critical failure conditions, in particular those single failures that may hamper or negate redundancies. The Failure Mode and Effects Analysis (FMEA) is one of the means to achieve this goal.

1.1.2 Scope of the Appendix

This Appendix describes the FMEA method and gives guidance as to how it may be applied by:

a) explaining basic principles

b) providing the procedural steps necessary to perform an analysis

c) identifying appropriate terms, assumptions, measures and failure modes, and

d) providing examples of the necessary worksheets.

1.1.3 Definition of FMEA

FMEA is a systematic process for identifying potential design and process failures before they occur, with the intent to eliminate them or minimise the risk associated with them.

1.1.4 FMEA principles

The FMEA is based on a single failure concept, under which each considered system at various levels of a system's functional hierarchy is assumed to fail by one realistic cause at a time. The effects of every postulated failure are analysed and classified according to their severity. Such effects may include secondary failures (or multiple failures) at other level(s). In general, the FMEA should verify that any active equipment (including computers, switchboards and the like) for which a failure mode may cause the loss of a safety-related function (e.g. propulsion or steering) is redundant and independent; the independence is to be verified up to the auxiliaries like power supplies, control systems, etc.. It may be accepted that static equipment (e.g. welded piping or cables) is out of the scope of the FMEA , but this should be specifically evaluated; e.g. flanged piping cannot be assumed to be fully static. A test programme should be drawn up to confirm the conclusions of FMEA.

1.1.5 Alternatives

While FMEA is suggested as one of the most flexible analysis techniques, it is accepted that there are other methods which may be used and which in certain circumstances may offer an equally comprehensive insight into particular failure characteristics.

1.2 Objectives

1.2.1 Primary objective

The primary objective of FMEA is to provide a comprehensive, systematic and documented investigation which establishes the critical failure conditions of systems related to the safety of the ship and its occupants: at least the ship propulsion, steering and power generation systems and those associated to the particular ship characteristics (e.g. Safe Return to Port or Gas-fuelled systems). Other systems may be added upon request by the Owner.

1.2.2 Aim of the analysis

The main aims of the analysis are to:

a) provide ship and system designers with information to check their proposed designs

b) provide the Owner with the results of a study into ship's selected systems failure characteristics so as to assist in an assessment of the arrangements and measures to be taken to limit the failure consequences within acceptable limits

c) provide an aid to the Owner's technical offices to update the operations, training , emergency and maintenance manuals requested by the applicable rules and regulations.

1.3 Sister ships

1.3.1 For ships of the same design and having exactly the same equipment and arrangement of the systems subjected to FMEA, one FMEA on any one of such ships may be sufficient, but each of the other ships are to be subject to the same FMEA trials.

1.4 FMEA basics

1.4.1 General

Before proceeding with a detailed FMEA into the effects of the failure of the system elements on the system functional output it is necessary to perform a functional failure analysis of the considered systems. In this way only systems which fail the func-tional failure analysis need to be investigated by a more detailed FMEA.

1.4.2 Operational modes

When conducting a system FMEA the following typical operational modes within the normal design environmental conditions of the ships are to be considered:

a) normal seagoing conditions at full speed

b) maximum permitted operating speed in congested waters

c) manoeuvring alongside
d) seagoing conditions in emergency, as defined in Sec 1, Sec 2, Sec 3 and Sec 4.

Other operational modes related to the specific ship's characteristics and service notations are to be specifically addressed

1.4.3 Functional interdependence

This functional interdependence of these systems is also to be described. As far as applicable, each of the systems to be analysed is assumed to fail in the following failure modes:

a) complete loss of function

b) rapid change to maximum or minimum output

c) uncontrolled or varying output

d) premature operation

e) failure to operate at a prescribed time

f) failure to cease operation at a prescribed time.

Depending on the system under consideration other failure modes may have to be taken into account.

1.4.4 Systems for which the FMEA can be waived

If a system can fail with failure modes and consequences that are clearly identifiable from the drawings, there is no need to conduct a detailed formal FMEA and the system's behavior is to be confirmed and documented by a practical test programme.

1.4.5 Redundant systems

Where a safety-related system is provided with a redundant system, the FMEA, inter alia, is to verify that:

a) the redundant system can be put into operation or can take over the failed system within the time-limit dictated by the most onerous operational mode without hazarding the ship;

b) the redundant system is completely independent of the system and does not share any common system element the failure of which would cause failure of both the system and the redundant system. As mentioned in [1.1.4], static common system elements may be acceptable.

Manual operations to align a redundant system are to be demonstrated to be realistically feasible, and the possibility of operator errors are also to be considered.

1.4.6 Software

Most modern shipboard systems are software-dependent to some extent. Software has a potential for common mode failure as normally there are redundant equipment or systems that use the same software. A software fault could therefore affect redundant PLC's or computers.

However, the desktop FMEA is not the appropriate tool to ascertain software failures. It is therefore essential,

and should be considered mandatory, for the manufacturers of such systems to demonstrate their quality assurance in developing their software.

Software functions should then be rigorously exercised during factory acceptance tests and FMEA trials tests.

2 FMEA performance

2.1 Procedure

2.1.1 The following steps are necessary to perform an FMEA:

a) to define the system to be analysed
b) to illustrate the interrelationships of functional elements of the system, by means of block diagrams
c) to identify all potential failure modes and their causes
d) to evaluate the effects on the system of each failure mode
e) to identify failure detection methods
f) to identify corrective measures for failure modes
g) to assess the probability of failures causing hazardous or catastrophic effects, where applicable
h) to document the analysis
i) to develop a test programme
j) to prepare FMEA report.

2.2 System definition

2.2.1 The first step in an FMEA study is a detailed study of the system to be analysed, through the use of drawings and equipment manuals, preferably collected in an overall narrative description of the system and its functional requirements and/or block diagrams; these are particularly needed when the FMEA is sent to the Society for the system's approval.

2.2.1 As a minimum, the following information is to be available:

a) general description of system operation and structure
b) functional relationship among the system elements
c) acceptable functional performance limits of the system and its constituent elements in each of the typical operational modes
d) system constraints.

2.3 Best Practice

2.3.1 Level of detail

The FMEA analysis is to be in sufficient depth until the participants are completely satisfied that all significant failure nodes and system responses to those failures are identified and confirmed; as a minimum, the behaviour of the interfaces and the auxiliaries upon failure is to be analysed, to ensure that the principles of SOLAS Reg. II-1/26.3 are met.
In general, an FMEA is to start from the overall system level and progress to the next level down, or subsystem lev-el, and so on down to the equipment item and component level.
However, at a certain level between overall system level and component level , if it can be shown that that a failure does not cause any further effect on the overall system, then it is not necessary to continue to the next level down.
For example, at sub-system level, it is generally acceptable to consider failure of equipment items and their functions, e.g. failure of a pump to produce flow or pressure head. It is not generally necessary to analyse the failure of the parts of the pump itself, unless their failure modes are of interest, i.e. may originate significantly different con-sequences on the overall system.

2.3.2 FMEA Team

In general, an FMEA is used to analyse systems that may include process pipes, electrical power supplies and electronics. Therefore, a proper FMEA requires a multi-disciplined team that include the stakeholders (at least representatives of yard, owner and Class society), persons having expertise in the various system aspects and skilled FMEA practitioners.
The depth of analysis of the system interfaces should also be sufficient to ensure the principles of SOLAS Reg. II-1/26.3 are met, and this is up to the judgement of the FMEA team.

2.4 Identification of failure modes, causes and effects

2.4.1 Failure mode

Failure mode is the manner by which a failure is observed. It generally describes the way the failure occurs and its impact on the equipment or system. As an example, a list of failure modes is given in Tab 1. The failure modes listed in Tab 1 can de-scribe the failure of any system element in sufficiently specific terms. When used in conjunction with performance specifications governing the inputs and outputs on the system block diagram, all potential failure modes can be thus identified and described. Thus, for example, a power supply may have a failure mode described as "loss of output" (29), and a failure cause "open (electrical)" (31).

Table 1: Example of failure mode list

1	Structural failure (rupture)
2	Physical binding or jamming
3	Vibration
4	Fails to remain in position
5	Fails to open
6	Fails to close
7	Fails open
8	Fails closed
9	Internal leakage
10	External leakage
11	Fails out of tolerance (high)
12	Fails out of tolerance (low)
13	Inadvertent operation
14	Intermittent operation
15	Erratic operation
16	Erroneous indication
17	Restricted flow
18	False actuation
19	Fails to stop
20	Fails to start
21	Fails to switch
22	Premature operation
23	Delayed operation
24	Erroneous input (increased)
25	Erroneous input (decreased)
26	Erroneous output (increased)
27	Erroneous output (decrease)
28	Loss of input
29	Loss of output
30	Shorted (electrical)
31	Open (electrical)
32	Leakage (electrical)
33	Other unique failure conditions as applicable to the system characteristics, requirements and operational constraints

2.4.2 System failure

A failure mode in a system element could also be the failure cause of a system failure. For example, the hydraulic line of a steering gear system might have a failure mode of "external leakage" (10). This failure mode of the hydraulic line could be-come a failure cause of the steering gear system's failure mode "loss of output" (29).

2.4.3 Top-down approach

Each system should be considered in a top-down approach, starting from the system's functional output, and failure is to be assumed by one possible cause at a time. Since a failure mode may have more than one cause, all potential independent causes for each failure mode are to be identified.

2.4.4 Delay effect when operating back-up systems

If major systems can fail without any adverse effect, there is no need to consider them further unless the failure can go undetected by an operator. To decide that there is no adverse effect does not mean just the identification of system redundancy. The redundancy is to be shown to be immediately effective or brought on line with negligible time lag. In addition, if the se-quence is: "failure - alarm - operator action - start of back up- back up in service", the effects of delay should be considered.

2.5 Failure effects

2.5.1 Concept

The consequence of a failure mode on the operation, function, or status of an equipment or a system is called a "failure effect". Failure effects on a specific sub-system or equipment under consideration are called "local failure effects". The evaluation of local failure effects will help to determine the effectiveness of any redundant equipment or corrective action at that sys-tem level. In certain instances, there may not be a local effect beyond the failure mode itself.

2.5.2 End effect

The impact of an equipment or sub-system failure on the system output (system function) is called an "end effect". End effects should be evaluated and their severity classified in accordance with the following categories:

a) catastrophic
b) hazardous
c) major
d) minor.

The definition of these four categories of failure effects is in [4]. Other severity scales may be agreed within the team.

2.5.3 Catastrophic and hazardous effects

If the end effect of a failure is classified as hazardous or catastrophic, back-up equipment is usually required to prevent or minimize such effect. For hazardous failure effects, corrective operational procedures may be generally accepted, but this is to be accepted by the team.

2.6 Failure detection

2.6.1 Detectable failures

The FMEA study in general only analyses failure effects based on a single failure in the system and therefore a failure detection means, such as visual or audible warning devices, automatic sensing devices, sensing instrumentation or other unique indications, is to be identified.

2.6.2 Non detectable failures

Where the system element failure is non-detectable (i.e. a hidden fault or any failure which does not give any visual or audible indication to the operator) and the system can continue with its specific operation, the analysis is to be extended to determine the effects of a second failure, which in combination with the first undetectable failure may result in a more severe failure effect e.g. hazardous or catastrophic effect.

2.7 Corrective measures

2.7.1 Back-up equipment response

The response of any back-up equipment, or any corrective action initiated at a given system level to prevent or reduce the effect of the failure mode of system element or equipment, is also to be identified and evaluated.

2.7.2 Corrective design provisions

Corrective design provisions are design features, at any system level, that nullify the effects of a malfunction or failure, such as controlling or deactivating system elements to stop generation or propagation of failure effects, activating back-up or standby items or systems. Corrective design provisions include:

a) redundancies that allow continued and safe operation
b) safety devices, monitoring or alarm provisions, which permit restricted operation or limit damage
c) alternative modes of operation.

2.7.3 Manual corrective actions

Provisions which require operator action to negate and mitigate the effects of the assumed failure modes are to be described. The possibility and effect of operator error is to be considered, when

evaluating the means to eliminate the local failure effects, if a corrective action or the activation of a redundancy requires operator intervention.

2.7.4 Acceptability of corrective action

It is to be noted that corrective responses acceptable in one operational mode may not be acceptable at another, e.g. a redundant system element that requires considerable time to be aligned, while meeting the operational mode "normal seagoing conditions at full speed" may result in an unacceptable effect in another operational mode, e.g. "maximum permitted operating speed in congested water".

2.8 Use of probability concept

2.8.1 General

A FMEA is not in itself a full risk analysis. For the purpose of demonstrating the compliance with SOLAS Reg. II-1/26.3 , the outcomes of the FMEA in terms of severity is sufficient. When the FMEA is carried out for other purposes, the probability considerations described in [4] may be needed, and in such cases acceptability criteria need to be defined.

2.8.2 Acceptance criteria

If corrective measures or redundancies as described in preceding paragraphs are not provided for any failure, as an alternative the probability of occurrence of such failure is to meet the criteria of acceptance defined up front. Typical acceptance criteria are as follows:

a) a failure mode which results in a catastrophic effect is to be assessed to be extremely improbable
b) a failure mode assessed as extremely remote is to not result in worse than hazardous effects
c) a failure mode assessed as either frequent or reasonably probable is not to result in worse than minor effects.

2.8.3 Data

Numerical values for various levels of probabilities are laid down in [4]. In areas where there is no statistical field data to deter-mine the level of probabilities of failure other sources can be used such as:
a) workshop test
b) history of reliability used in other areas under similar operating conditions
c) mathematical models if applicable
c) recognized databases.

2.9 Documentation

2.9.1 Worksheet

It is helpful to perform FMEA on worksheets. Tab 2 shows an example of worksheet. Other formats may be agreed by stake-holders.

2.9.2 Worksheet organization

The worksheets are to be organized to first display the highest system level and then proceed down through decreasing sys-tem levels.

Table 1: FMEA Worksheet

Name of system : Mode of operation : Sheet No : Date : Name of analyst :							References: System block diagram: Drawings:				
Equipment name or number	Function	Ident. No.	Failure mode	Failure cause	Failure effect		Failure detection	Corrective action	Severity of failure effect	Probability of failure (if applicable)	Remarks
					Local effect	End effect					

3 TEST AND REPORTING

3.1 Test program

3.1.1 FMEA validation test

An FMEA test programme is to be drawn up to prove the conclusions of FMEA. It is recommended that the test programme is to include all systems or system elements whose failure would lead to:

a) major or more severe effects
b) restricted operations
c) any other corrective action.

For equipment where failure cannot be easily simulated on the ship, the results of other tests can be used to determine the effects and influences on the systems.

3.1.2 Further investigations

The trials are also to include investigations into:

a) the layout of control stations with particular regard to the relative positioning of switches and other control devices to ensure a low potential for inadvertent and incorrect crew action, particularly during emergencies and the provision of interlocks to prevent inadvertent operation for important system operation
b) the existence and quality of the craft's operational documentation with particular regard to the pre-voyage checklists. It is essential that these checks account for any unrevealed failure modes identified in the failure analysis
c) the effects of the main failure modes as prescribed in the theoretical analysis.

3.2 Reporting

3.2.1 General

The FMEA report is to be a self-contained document with a full description of the craft, its systems and their functions and the proposed operation and environmental conditions for the failure modes, causes and effects to be understood without any need to refer to other plans and documents not in the report. The analysis assumptions and system block diagrams are to be included, where appropriate.

The report is to contain a summary of conclusions and recommendations for each of the systems analysed in the system failure analysis and the equipment failure analysis. It is also to list all probable failures and their probability of failure where applicable, the corrective actions or operational restrictions for each system in each of the operational modes under analysis. The report is to contain the test programme, reference any other test reports and the FMEA trials.

4 PROBABILISTIC CONCEPT

4.1 General

Different undesirable events may have different orders of acceptable probability. In connection with this, it is convenient to agree on standardized expressions to be used to describe the probabilities of various occurrences, i.e. to perform a qualitative ranking process.

4.2 Occurrences

4.2.1 Occurrence

Different undesirable events may have different orders of acceptable probability. In connection with this, it is convenient to agree on standardized expressions to be used to describe the probabilities of various occurrences, i.e. to perform a qualitative ranking process.

4.2.2 Failure

Failure is an occurrence in which a part, or parts, of a system fail. A failure includes:

a) a single failure independent failures in combinations within a system, and
b) independent failures in combinations involving more than one system, taking into account:
    1) any undetected failure that is already present
    2) such further failures as would be reasonably expected to follow the failure under consideration, and
c) common cause failure (failure of more than one component or system due to the same cause).

Note 1: In assessing the further failures which follow, account should be taken of any resulting more severe operating conditions for items that have not up to that time failed.

4.2.3 External event

An external event is an occurrence which has its origin outside the craft (e.g., waves).

4.2.4 Error

Error is an occurrence arising as a result of incorrect action by the operating crew or maintenance personnel.

4.3 Probability of occurrences

4.3.1

The likelihood of an undesired event. The scale and definition of the probabilities are to be agreed by the team up front. In the following a typical set of definitions is presented.

4.3.2 Frequent

Likely to occur frequently.

4.3.3 Reasonably probable

Unlikely to occur often but which may occur several times during the total operational life of a particular ship.

4.3.4 Remote

Unlikely to occur to every ship but may occur to a few ships of a type over the total operational life of a number of ship of the same type.

4.3.5 Extremely remote

Unlikely to occur when considering the total operational life of a number of ships of the type, but still judged to be possible.

4.3.6 Extremely improbable

Extremely improbable is one which is so extremely remote that it should not be considered as possible to occur.
Typical numerical values are illustrated in the following Table 3.

Table 3

Frequent	More than 10^{-3}
Reasonably probable	10^{-3} to 10^{-5}
Remote	10^{-5} to 10^{-7}
Extremely remote	10^{-7} to 10^{-9}
Extremely improbable	Whilst no approximate numerical probability is given for this, the figures used should be substantially less than 10^{-9}

4.4 Severity of the consequences

4.4.1 Severity

The magnitude of the consequences of an undesired event. The scale and definition of the effects are to be agreed by the team up front. In the following a typical set of definitions is presented.

4.4.2 Minor effect

Minor effect is an effect which may arise from a failure, an event, or an error, which can be readily rectified by the operating crew; it may involve for example:

a) a small increase in the operational duties of the crew or in their difficulty in performing their duties, or
b) a moderate degradation in handling characteristics, or
c) slight modification of the permissible operating conditions.

4.4.3 Major effect

Major effect is an effect which produces, for example:

a) a significant increase in the operational duties of the crew or in their difficulty in performing their duties which by itself should not be outside the capability of a competent crew provided that another major effect does not occur at the same time, or
b) significant degradation in handling characteristics, or
c) significant modification of the permissible operating conditions, but will not remove the capability to complete a safe journey without demanding more than normal skill on the part of the operating crew.

4.4.4 Hazardous effect

Hazardous effect is an effect which produces:

a) a dangerous increase in the operational duties of the crew or in their difficulty in performing their duties of such magnitude that they cannot reasonably be expected to cope with them and will probably require outside assistance, or
b) dangerous degradation of handling characteristics, or
c) dangerous degradation of the strength of the ship, or
d) marginal conditions for, or injury to, occupants, or
e) an essential need for outside rescue operations.
e) a loss of propulsion and/or steering.

4.4.5 Catastrophic effect

Catastrophic effect is an effect which results in the loss of the craft and/or in fatalities.

4.5 Risk

4.5.1

When each failure mode should be assigned a value for frequency of the failure occurring and a value for the con-sequence, or severity, of each failure, the associated risk is:
Risk = Frequency x Consequence

4.5.2 Risk matrix

When the FMEA entries are assigned probability and severity , the results should be ranked by means of a risk matrix agreed up front, like that shown in Table 4 for illustrating purposes.

Table 4

Likelihood	Severity levels			
	1 Insignificant	**2 Marginal**	**3 Critical**	**4 Catastrophic**
5: Frequent	Undesirable	Intolerable	Intolerable	Intolerable
4: Probable	Tolerable	Undesirable	Intolerable	Intolerable
3: Occasional	Tolerable	Undesirable	Undesirable	Intolerable
2: Remote	Negligible	Tolerable	Undesirable	Undesirable
1: Improbable	Negligible	Negligible	Tolerable	Tolerable

5 FMEA MANAGEMENT

5.1 General

5.1.1

The FMEA report should be revisited as a result of changes made to the system during the life of the system and in the light of any information gathered at a later date that was not available at the time of the FMEA.
Any safety related equipment changes to the system should be analysed to identify whether they have an impact on the FMEA. Any identified changes should be addressed on an on-going basis but not later than the trials to be per-formed in the next annual survey.
AIP should be consistent with the following general

5.2 FMEA trials Plan

5.2.1 Occurrence

The FMEA trials are a series of controlled failure mode tests which are intended to prove the findings of the desktop FMEA and, where there are any doubts about any failure modes from the desktop analysis, eliminate these doubts by carrying out onboard testing in a safe and practical manner.

- FMEA testing should be a structured and well co-ordinated exercise to demonstrate:
- the redundancy concept;
- the effectiveness of system protection functions;
- stability of the system under the full range of load/operational conditions;
- monitoring functions;
- degraded and failure conditions.

For this to be achievable, the complete system should have undergone full commissioning test process and be fully operational, particularly alarm and event logging. A suitable number of qualified personnel need to be present for witnessing the tests.

All participants should review the test procedures so that the method and expected failure effects are well understood beforehand.

It is to be ensured that FMEA trials results are properly recorded and fed back into the FMEA document to reflect the trial findings where applicable.