Tasneef®
Life Environmentally Optimized

Guide to Perform the Failure Mode and Effect Analysis (FMEA) for High Speed Craft (HSC)

Effective from 1 January 2016

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 authorized 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 Governments.

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 reinstatement. 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 the 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 part 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 certificate 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 seaworthiness,

structural integrity, quality or fitness for a particular purpose or service of any Ship, structure, 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 certification 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, the 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 statutory 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 authorization 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

Part C - Examples

PREMISE

P.1 GENERAL

The scope of this guide is to provide interpretations of the requirements concerning the FMEA (Failure Mode and Effect Analysis) for high speed craft as well as to provide indications on how to carry out an FMEA acceptable to TASNEEF. The two aspects are dealt with in parts A and B of this document.

Part C contains some simple examples of the application of the various steps of the analysis to actual cases.

P.2 FIELD OF APPLICATION

This guide applies to high speed craft for the purpose of carrying out the FMEA as prescribed by the Rules for the Construction and Classification of High Speed Craft (hereafter referred to simply as "HSC Rules").

The FMEA is required for category A and B passenger craft and cargo craft before they enter into service or before the High Speed Craft Safety Certificate is issued for the first time (chapter 1 - 1.5 of the HSC Rules).

The FMEA is to be integrated in the design process of the craft, so that any modifications which may result from the FMEA may be incorporated into the design with minimal changes and before construction has advanced to a stage where changes incur unreasonable expenditure.

The analysis should at least address the following systems (annex 4 - 3.1 of the HSC Rules):
* directional control system (chapter 5 - 5.2.5 of the HSC Rules)
* machinery systems and their associated controls (chapter 9 - 9.1.10 of the HSC Rules)
* those programmable electronic systems where manual intervention to avert a danger is not possible (chapter 11 - C.11.0.1.8 of the HSC Rules)
* electrical system (chapter 12 - 12.1.1 of the HSC Rules)
* stabilisation system (chapter 16 - 16.2.6 of the HSC Rules).

When conducting the analysis, the following operational modes should be considered (annex 4 - 4.2 of the HSC Rules):
* normal seagoing conditions at full speed;
* maximum permitted operating speed in congested waters; and
* manoeuvring alongside.

PART A - INTERPRETATION OF RULE REQUIREMENTS

1. GENERAL

In chapters 5, 9, 11, 12 and 16, the HSC Rules prescribe that the main systems of a high speed craft be subject to a FMEA (in accordance with the requirements in annex 4 of the above rules).

2. DEFINITIONS

"***Category A craft***" is any high speed passenger craft:

(1) operating on a route where it has been demonstrated to the satisfaction of the flag and port States that there is a high probability that in the event of an evacuation at any point of the route, all passengers and crew can be safely rescued within the least of:
   - the time to prevent persons in survival craft from exposure causing hypothermia in the worst intended conditions,
   - the time appropriate with respect to environmental conditions and geographical features of the route, or
   - 4 h; and

(2) carrying not more than 450 passengers.

"***Category B craft***" is any high speed passenger craft, other than a category A craft, with machinery and safety systems arranged such that, in the event of damage disabling any essential machinery and safety systems in one compartment, the craft retains the capability to navigate safely.

"***Cargo craft***" is any high speed craft other than passenger craft, which is capable of maintaining the main functions and safety systems of unaffected spaces, after damage in any one compartment on board.

"***Corrective actions***" are actions, already foreseen by the designer and/or normally used in the operational measures, to prevent or reduce the effect of the failure of a system element or equipment.

"***Corrective measures***" are actions which, as a result of the FMEA study, are implemented to prevent or reduce the effect of the failure mode of a system element or equipment.

"***Failure mode***" is the effect by which a failure is observed.

"***Failure effect***" is the consequence of a failure mode in terms of the operation, function or status of a system.

"***Risk***" is the combination of the probability of occurrence and severity of effects of a failure mode.

3. SCOPE AND DOCUMENTATION

The main aims (annex 4 - 2.2 of the HSC Rules) of undertaking the analysis are to:

* provide TASNEEF with the results of a study concerning a craft's failure modes and effects so as to assist in assessing the levels of safety for the craft's operation;
* provide craft operators with data to generate comprehensive training, operational and maintenance programmes and documentation; and
* provide craft and system designers with data to assess their proposed designs.

The scope of the FMEA is to demonstrate that the risks induced by failure of a system, subsystem or component are within acceptable limits due to either redundancy or corrective measures.

Furthermore, it shall be proved that:

* for an A craft, the consequences of an event requiring the evacuation of the craft are such that the craft must be able to stay afloat as long as necessary to enable its evacuation;
* for a B craft, the consequences of damage disabling any essential machinery and safety systems in one compartment are such that the craft retains the capability to navigate safely;
* for a cargo craft, the consequences of damage in any compartment on board are such that the main functions and safety systems of spaces unaffected by the damages are maintained.

The above is to be proved by executing a vulnerability analysis showing the ability of the craft to withstand external events (e.g. fire, flooding) which could impair the integrity of the essential craft compartments.

The purpose of an FMEA is to identify single component and system failure modes and relevant potential effect(s) on the craft. This analysis typically generates recommendations for improving component or system reliability, hence craft safety.

The analysis should be (annex 4 - 2.1 of the HSC Rules) comprehensive, systematic and documented so as to:

* determine the important failure conditions of the craft,
* assess their significance with regard to the safety of the craft, its occupants and the environment.

"Documented" means that a self-supporting report is to be issued in accordance with the requirements in annex 4 - 16.1 of the HSC Rules. This report is to be submitted to the Head Office and shall include:

* a description of the craft, its systems and their functions;
* a description of operation and environmental conditions and any other necessary information to understand failure modes, causes and effects of main systems without the need of any other documentation not attached to the report;
* a description of the assumptions of the analysis;
* system block diagrams, where applicable;
* a list of the most probable failures and, where applicable, associated probability of failure;
* the list of corrective actions/operational restrictions and recommendations for each system;
* the worksheet documenting FMEA;
* an FMEA test programme.

The final stage of the analysis will be:

* full-scale trials simulating the possible equipment failures (annex 8 - 4 of the HSC Rules);
* the report of FMEA trials;

* the inclusion in the craft operating manual of any corrective action or limitation in the craft operations which, according to FMEA results, are necessary to keep risks within the acceptable limits (chapter 17 - 17.5.1 of the HSC Rules).

4. LEVEL OF ANALYSIS AND ACCEPTANCE CRITERIA

4.1 General

The FMEA is based on a single failure concept, i.e. each system is assumed to undergo a significant failure by one probable cause at a time (annex 4 - 1.5 of the HSC Rules).

In case one cause results in more than one failure (common cause failure), all the resulting failures have to be considered together. In case the occurrence of a failure leads automatically to further failures, all those failures have to be considered.

In the analysis, a number of postulated failure modes should be examined systematically with respect to their effects, both local and on the global craft, severity and probability of occurrence. The failure modes describe deviations from normal operating conditions, such as a complete or partial loss of function, uncontrolled output, or failure to operate at a prescribed time. During the analysis these postulated failure modes should be applied to the system under consideration. The following steps of the analysis should be sought:

- Failure cause
- Local effect
- Effect on the global craft
- Failure detection
- Corrective action.

4.2 Levels of analysis

Two levels of analysis are defined (annex 4 - 4 of the HSC Rules):

- 1st level (system FMEA): the analysis is carried out on a system level: every function of each of the craft's main systems is analysed with respect to possible failure modes, causes and effects on the entire craft for all typical operational modes (listed in P2). This kind of analysis is therefore also referred to as functional failure analysis (annex 4 - 4.1 of the HSC Rules).
- 2nd level (detailed FMEA): the analysis is carried out at a lower hierarchical level, examining the components or units of a system; compared with the system FMEA, this 2nd level analysis goes into more detail: each conceivable mode in which a component or unit can fail with respect to its intended function is analysed. The 2nd level analysis is prescribed (annex 4 - 4.4 of the HSC Rules) for the systems which failed the 1st level, i.e.:

  ⇒ the individual failure of which can cause hazardous or catastrophic effects, and

  ⇒ where the provided redundancy does not meet the criteria in the Rules (annex 4 - 4.5 of the HSC Rules), and

  ⇒ the probability of occurrence acceptance criteria (annex 4 - 13 of the HSC Rules) are not met.

  A detailed analysis may also be necessary for specific systems (annex 4 - 5 of the HSC Rules) which may include those that have a significant influence on the safety of the craft and its occupants requiring an investigation at a deeper level than a 1st level system functional failure analysis. These systems may be those which have been specifically designed or adapted for the craft, such as the craft's electrical and hydraulic systems.

Functional (1st level) and detailed (2nd level) analyses are sketched in the flow charts in figures 1 and 2.

4.3 Severity of failure effects

The following four categories of severity of failure effects are considered (annex 4 - 10.2 of the HSC Rules) with respect to the effects on the occupants and the craft itself (annex 3 - 2.3 of the HSC Rules):

* an effect is considered **catastrophic** if it results in the loss of the craft and/or in fatalities;

* an effect is considered **hazardous** if it produces:
  1. a dangerous increase in the operational duties of the crew or in the difficulty in performing their duties of such magnitude that they cannot reasonably be expected to cope with them and which probably requires outside assistance; or
  2. dangerous degradation of handling characteristics; or
  3. dangerous degradation of the strength of the craft; or
  4. marginal conditions for, or injury to, occupants; or
  5. an essential need for outside rescue operations.
* an effect is considered **major** if it produces:
  1. 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
  2. significant degradation in handling characteristics; or
  3. significant modification of the permissible operating conditions, but which will not remove the capability to complete a safe journey without demanding more than normal skill on the part of the operating crew.
* an effect is considered **minor** if it arises from a failure, an event or an error which can be readily compensated for by the operating crew; it may involve:
  1. a small increase in the operational duties of the crew or in their difficulty in performing their duties, or
  2. a moderate degradation in handling characteristics, or
  3. a slight modification in the permissible operating conditions.

The assessment of the severity of failure effects may differ for craft of category A and B. For category A craft, the assumption can be made that external assistance will be available after a period no longer than 4 hours. Such an assumption is not allowed for category B craft. Therefore, failure resulting in the need for external assistance will be more critical for category B craft.

4.4 Corrective actions, corrective measures and redundancy

Both **corrective actions and measures** are actions to prevent or reduce the effect of the failure mode of a system element or equipment (annex 4 - 12.1 of the HSC Rules) and can be "corrective design provisions" or "corrective operational procedures". The difference is that while corrective actions are already foreseen at the design stage of the craft, corrective measures are implemented as a result of the FMEA study.

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

1. redundancies that allow continued and safe operation;
2. safety devices, monitoring or alarm provisions, which permit restricted operation or limit damage;
3. alternative modes of operation (i.e. at reduced speed, with only one engine, etc.).

Corrective operational procedures are provisions which require operator action to circumvent or mitigate the effect of a failure.

For failure modes causing hazardous effects corrective measures may be accepted in lieu of redundancy (annex 4 - 1.5 of the HSC Rules).

Redundancy is a corrective design provision consisting in the installation of back-up equipment. An adequate **redundant system** must be able to:

1) enter into operation or take over the failed system within the time-limit dictated by the most onerous operational mode (defined in P.2) without endangering the craft;
2) be completely independent from the main system and not share any common system element the failure of which would cause failure of both the system and the redundant system. Common system element may be acceptable if the probability criteria (annex 4 - 13 of the HSC Rules) are met;
3) be located at a sufficient distance from the main system so that a fire or explosion of the main system does not prevent the redundant system from operating (e.g. for inadequate conditions of temperature and/or pressure); and

4) have an alternative power source readily available with regard to the requirement of 1), in case the redundant system shares the same power source as the system

4.5 Probability of occurrence of a failure

The probability of occurrence of a failure ranges from the qualitative expressions "frequent" to "extremely improbable". Numerical values associated with these qualitative expressions are (annex 3 - 3 of the HSC Rules):

	Probability of occurrence P (on an hourly basis)	For instance, assuming 2000 hours of craft operation every year
Frequent	more than 10^{-3}	more than 2 occurrences on a craft every year ($P \geq 10^{-3}$)
Reasonably probable	10^{-3} to 10^{-5}	1 occurrence on a craft every 5 years ($P = 10^{-4}$)
Remote	10^{-5} to 10^{-7}	1 occurrence on 5 craft every 20 years ($P = 5\ 10^{-6}$)
Extremely remote	10^{-7} to 10^{-9}	1 occurrence on 2500 craft every 20 years ($P = 10^{-8}$)
Extremely improbable	less then 10^{-9}	1 occurrence on 250000 craft every 20 years ($P = 10^{-10}$)

The probability of occurrence may be determined on the basis of operational experience on similar craft. When no operational data are available, other sources may be used, such as workshop tests or numerical simulations. When experience or data is available for basic events leading to the failure under consideration (top event), Fault Tree Analysis may be helpful to evaluate the probability

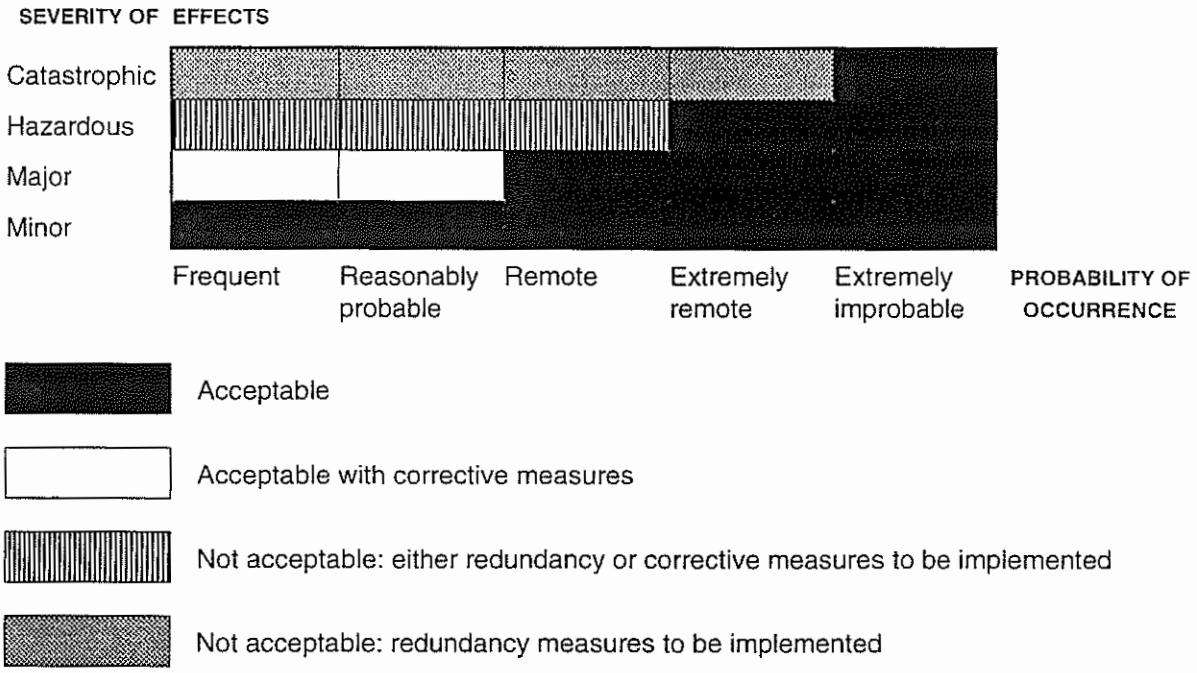
4.6 Acceptance criteria

Risk is defined as the combination of the probability of occurrence and severity of effects of a failure mode.

The acceptability of a failure mode is to be assessed against the risk, which can be either acceptable or not acceptable according to the following acceptance criteria (annex 4 - 13.1 of the HSC Rules):

1) a failure mode which results in a catastrophic effect is acceptable if it has been assessed to be extremely improbable;
2) a failure mode assessed as extremely remote should not result in worse than hazardous effects; and
3) a failure mode assessed as either frequent or reasonably probable should not result in worse than minor effects.

The above acceptance criteria can be represented by means of the following acceptance matrix:



4.7 Steps of the analysis

Summarising, the functional failure analysis (1st level FMEA) of a system consists in listing the system failure modes and for each failure mode:

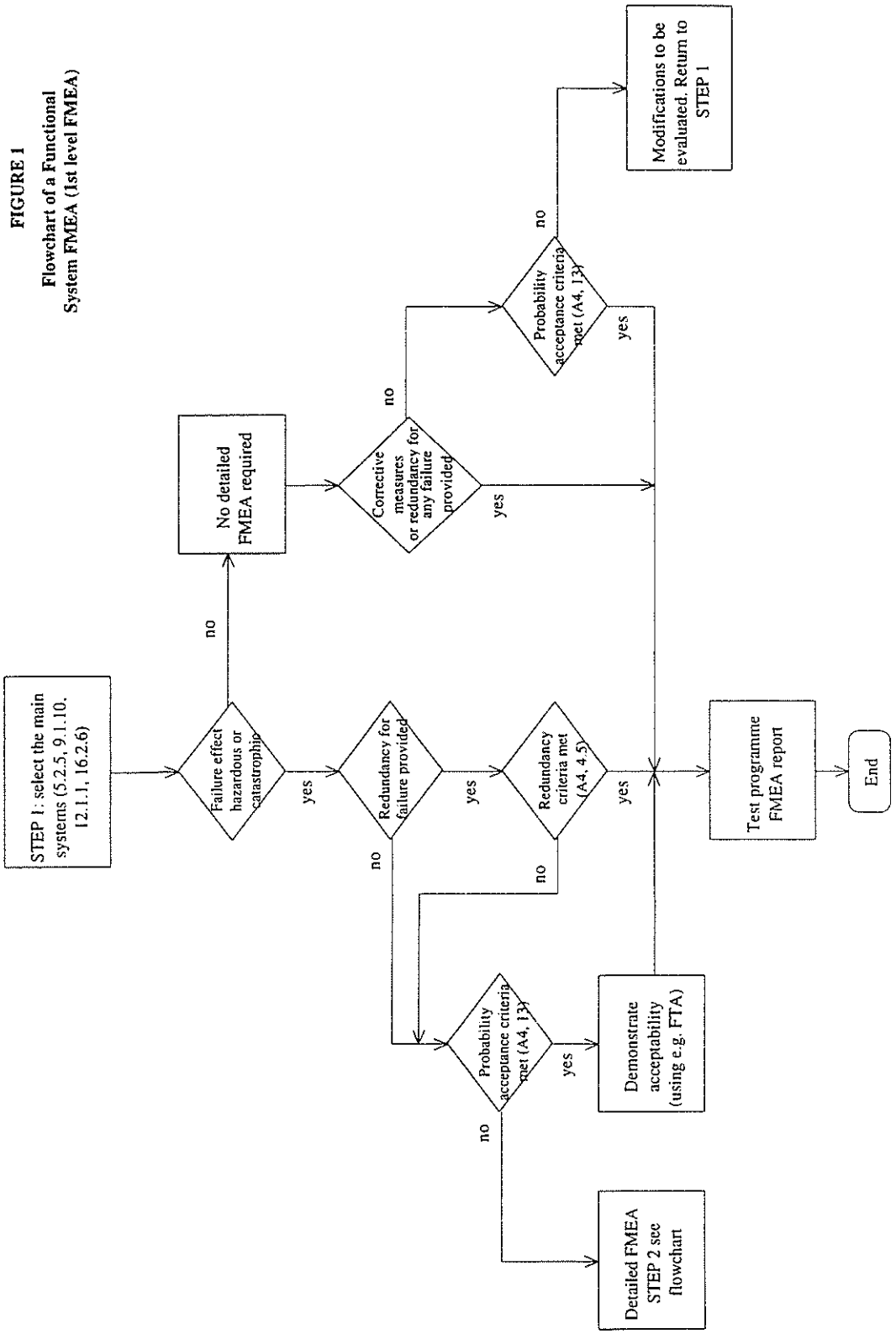
1. assess the severity of failure effect; if the failure mode results in minor effects, consider it acceptable and stop;
2. if the redundancies of the system with respect to the failure mode are considered adequate, stop;
3. assess the probability of occurrence of the failure mode; if it is not possible to estimate a value of probability occurrence, implement redundancy or corrective measures in order to mitigate the effects to minor and stop;
4. use the acceptance matrix; if the risk can be considered acceptable, stop;
5. if the risk is unacceptable, implement measures to limit the severity of effect and/or reduce the probability of occurrence, e.g. by improving means for detection, eliminating failure causes, providing an adequate level of redundancy etc.; if after implementation of these measures, the risk is assessed as acceptable, stop;

For those failure modes resulting in not acceptable risks or when corrective measures are difficult to identify or too onerous, a **2nd level FMEA** of the subsystems or components involved should be performed in order to identify the necessary redundancy measures to be implemented.

A 2nd level FMEA should also be carried out when there are clear grounds that a certain system component is critical for the system safety, i.e. it could hide a single point failure for the system.

The above-mentioned steps are sketched in the flow chart in figure 3.

FIGURE 1
Flowchart of a Functional System FMEA (1st level FMEA)



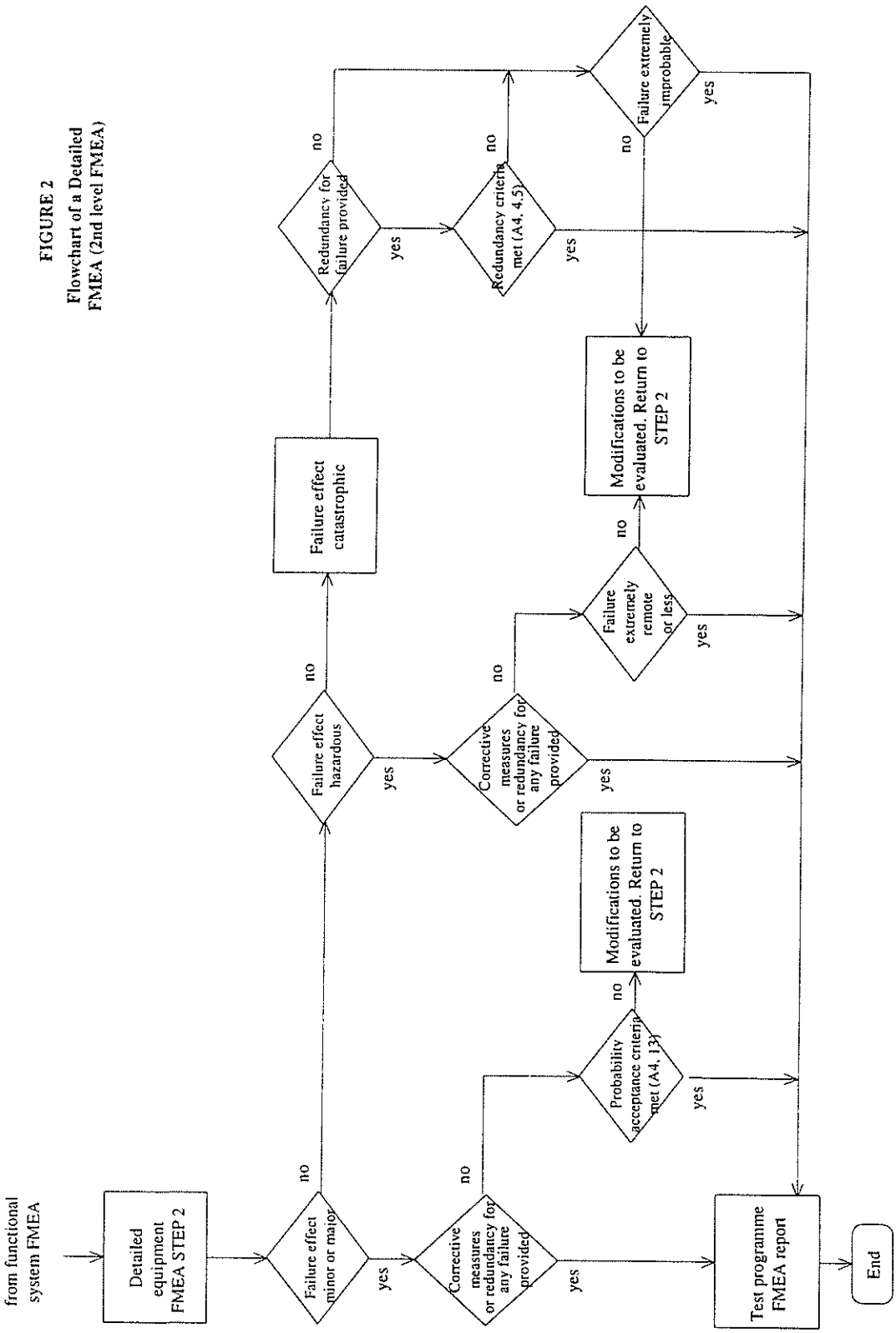
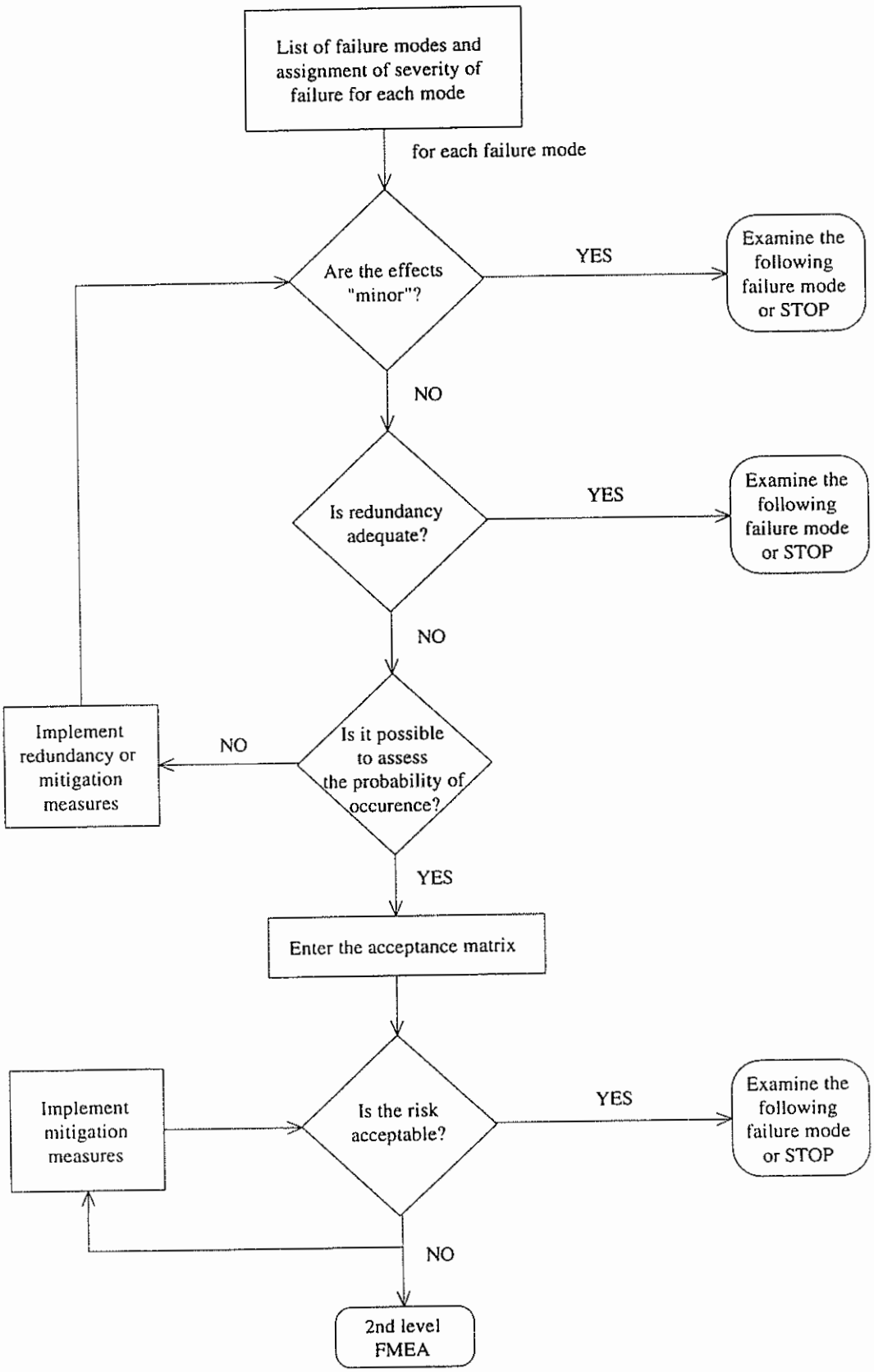


FIGURE 2
Flowchart of a Detailed FMEA (2nd level FMEA)

FIGURE 3

Functional failure analysis (1st level FMEA) of a system



PART B - PROPOSED METHODOLOGY

1. INFORMATION NEEDED

1.1 General

For both first and second level analyses the same kind of information and method of presentation are required.

1.2 Description of the craft

The description of the craft consists of a general narrative description of the craft, including:

i) its overall characteristics (such as the type of craft, length, gross tonnage, number of passengers);

ii) a general arrangement plan showing the main systems (such as propulsion plant, electrical system, stabilisation system, control systems, emergency systems);

iii) block diagram representing the relationship between the main systems (the use of the block diagram can simplify both i) and ii) above);

iv) operative profile of the craft, in order to enable identification of the system functional requirements for each typical operational mode of the craft.

An example of the description of a passenger ro-ro high speed craft is given in Part C, 1.1 (Example 1).

A description of the behaviour of the craft under external events (e.g. fire, flooding) which could impair the integrity of its essential compartments (vulnerability analysis) is also requested.

1.3 Narrative description of the systems

For each of the main systems subject to the FMEA (see P.2) the following information should be provided:
a) description of system;
b) description of system operation and control;
c) environmental conditions;
d) list of reference design drawings and documents;

with the aim of describing each component and equipment in order to support the identification of the failure modes which may occur and the relevant effects on safety of the craft.

a) The description of the system needs to include the following particulars:
   - the different system elements with their characteristics, functions and operating modes;
   - the logical connections between elements;
   - system relationships, dependencies, or interconnections with auxiliary or other systems and human interfaces;
   - redundancies;
   - input and output of the system and its elements.

b) The different operating conditions of the system should be specified, as well as the changes in the configuration of the system and its elements during the different operational modes of the craft. The definition of functional characteristics and operational limits of each system is essential to link the effects of failures of the single system to the entire craft.

   Information needs to include the following items:
   - the time available for corrective action subsequent to a failure before serious consequences may occur to the craft;
   - interfaces and interactions between operators;
   - control of the system during the different operational modes of the craft.

c) The environmental conditions (e.g. intake air temperature, ambient temperature, humidity, etc.) which affect the performance of the system should be specified.

At the design stage not all the information is normally available and therefore approximations and assumptions will be needed. As the project progresses, the new data will have to be justified and the FMEA modified to allow for new information or changed assumptions or approximations.

An example of description of the stabilisation system is given in Part C, 1.2 (Example 2).

The following sheet may be used to describe each identified element of the system:

CRAFT:	FMEA level: .....
SYSTEM NAME	
ELEMENT NAME	
REFERENCE	
FUNCTION	
CHARACTERISTICS	
OPERATING MODES: • NORMAL • ABNORMAL	
INPUT/OUTPUT	
RELATED SYSTEMS	
REDUNDANCY	
CORRECTIVE ACTIONS	

An example of a sheet for the main control unit of the stabilisation system is given in Part C, 1.3 (Example 3).

1.4 Block diagram

A block diagram is necessary to technically understand the system's functions and prepare for the subsequent analyses.

A block diagram is a representation of the relevant information on the system, in particular relationships between the system elements and their functional interdependencies. This allows the functional failures to be tracked through the system.

If substantial differences exist, a separate block diagram should be developed for each operational mode.

As a minimum, the block diagram should contain the following:

- breakdown of the system into blocks representing major subsystems/elements (e.g. for machinery system: main propulsion, fuel supply, pump);
- identification numbers by which each element is consistently referenced throughout the whole FMEA;
- indication of functional relationship between the system elements including power and signal interactions between the blocks;
- all appropriately labelled inputs and outputs to/from the blocks, including those to/from other systems (e.g. mechanical power (MP), electrical power (EP), hydraulic power (HP) and electrical signal (ES));
- indication of all engineering features which provide "fail-safe" measures (e.g. redundancies, alternative signal paths).

An example of a block diagram of the stabilisation system is given in Part C, 1.4 (Example 4).

1.5 Identification of a system's boundaries

When describing a system subject to the FMEA, it is necessary to clearly define:

- which elements are part of the system; and
- which are the points of contact of the system with other systems.

This definition, which can be indicated as "identification of the system's boundaries", should derive from functional rather than physical divisions, i.e. related to the function that the system is intended to perform in the

craft. A single element can be considered in two or more systems; in this case it is necessary to highlight exactly the functions attributed to that element in each system.

It is important to stress that the identification of boundaries implies the definition of the relationship between the systems' elements with other systems. This implies the inclusion of "loss of input from other systems" (e.g. loss of electrical power or signal) among the potential causes of failure of a certain element and "loss of output to other systems" among the consequences of the element failure.

Unless a specific FMEA of the control system is carried out, the control units and equipment have to be considered as part of the system under analysis. Generation and distribution of electrical power are not to be modelled as they are to be analysed in the electrical system FMEA.

For the sake of clarity, an example of definition of boundaries is given in Part C, 1.5 (Example 5).

2. SYSTEM ANALYSIS (1st level - functional failure analysis)

2.1 General

Functional failure analysis is a systematic and comprehensive assessment of the system's functions to identify potentially serious failure conditions which the system can cause or contribute to. It is concerned with the operational vulnerabilities of the systems rather than with detailed hardware analysis.

Where adequate redundancies are identified, the consequences need not be studied any further (NC - Not Critical). Where the considered failure mode does not meet with the criteria (i.e. annex 4 - 4.4, redundancy in annex 4 - 4.5, probability in annex 4 - 13 of the HSC Rules), a detailed analysis is to be carried out.

Note: *When considering a category B craft where a rather high level of redundancy is expected, the number of detailed analyses may be limited.*

In summary, the steps to be followed for this functional failure analysis (1st level) are listed in annex 4 - 6.1.1 to 6.1.4 of the HSC Rules:

- define the system to be analysed;
- illustrate the interrelationship of the functional elements of the system, by means of block diagrams:
- identify all potential failure modes and their causes;
- evaluate the effects on the system for each failure mode.

As a result of a 1st level analysis, the list of hazardous/catastrophic failure effects should be produced. Those failures for which either redundancy or corrective measures are foreseen can be accepted. For the remaining ones, a 2nd level analysis is required if their probability of occurrence cannot be classified as extremely improbable or remote. The evaluation of the failure probability of occurrence, when allowing avoidance of a 2nd level analysis, is to be justified by performing additional analyses.

2.2 Worksheets

There are wide variations in the manner in which an FMEA is conducted and presented. However, the analysis should be done by using standard worksheets that contain the essential information which can be developed and extended to suit the particular system to which it is applied.

After having developed system block diagrams, where practicable, the analysis can be performed (see annex 4 - 14.1 of the HSC Rules) by using the worksheet shown in annex 4 - Appendix 2 of the HSC Rules (Table 1 hereto attached). The worksheet is defined by the following columns:

Equipment name or number	Name of the considered component
Function	Purpose of the component in the system
Identification number	Sequential numbers to identify the item and its failure (x-y-z) where: x identifies FMEA worksheet set y identifies the subsystem or component z identifies equipment function, failure mode or failure causes
Failure mode	Type of failure, is the effect by which a failure is observed
Failure cause	Causes leading to type of failure
Local failure effect	Consequences on the system of the failure mode
End failure effect	More general consequences of the failure mode related to the craft
Failure detection	Means by which failure can be detected
Corrective action	Any corrective action already foreseen to reduce the failure effects
Severity of failure effect	Ranking of end effect in accordance with the proposed categories (see Part A, 4.3)
Probability of failure (if applicable)	Probability of failure occurring. Probability evaluation is carried out only when corrective measures or redundancy are not provided
Remarks	Explanation for the ranking of failure severity and probability, recommendations including corrective measures to be implemented, and general comments such as the reasons for having excluded certain failure effects or the necessity to carry out some tests or checks

The column relevant to the probability of failure is filled only when this information is necessary to meet the risk acceptance criteria.

An example of a worksheet of the stabilisation system is given in Part C, 2.1 (Example 6).

2.3 Failure modes

The procedures for identifying failure modes, their causes and effects can be effectively enhanced by the preparation of a list of the characteristics of the system, including the following:

* use of the system;
* particular system element involved;
* mode of operation;
* pertinent operational specifications;
* time constraints;
* environment.

The definition of failure modes, failure causes and failure effects depend on the level of analysis. As the analysis progresses, failure effects identified at a lower level may become failure modes at a higher level. Similarly, failure modes at a lower level may become failure causes at a higher level.

A list of general failure modes is given in annex 4 - 4.3 of the HSC Rules. The following may be considered:

* complete loss of function;
* rapid change to maximum or minimum input;
* uncontrolled or varying output;
* premature operation;
* failure to operate at a prescribed time; and
* failure to cease operation at a prescribed time.

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

Examples of failure modes of components of different systems are given in Part C, 2.2 (Example 7).

2.4 Failure causes

Since a failure mode can have more than one cause, all potential independent causes associated with each possible failure mode should be identified and described in order to estimate their probability of occurrence, identify secondary effects and devise recommended corrective actions.

However, it may be time saving to first assess the effects of failure modes and then to identify the causes. Should the effects be minor, a listing of all the causes may not be very helpful.

The failure causes within the adjacent systems should also be considered in terms of loss of input coming from another system.

A more specific definition of failure causes can be developed as follows:

Type of failure cause	Examples
Equipment failure	Cracked/fractured Blockage Failure to open and/or close Leakage
Loss of input	Fuel pipe failure Blackout Loss of hydraulic power Loss of electrical signal
Maintenance problems	Omitted maintenance operation Erroneous maintenance operation Procedural error Off-line equipment failure
Change of environmental conditions	Temperature Humidity Vibration Corrosion
Erroneous action	Omitted action Erroneous control Procedural error

Examples of failure causes for components of different systems are given in Part C, 2.3 (Example 8).

Shipping accidents are influenced to a large extent by human error. The human error element should therefore be taken into account whenever assessing failure causes. Systematic methods studying and taking into account human errors, although neither rigorous nor fully comprehensive, may be useful.
Human error itself is influenced by a variety of factors, e.g. the environment to which the operator is exposed, the operator's qualification, man-machine interface etc.
For the purpose of human error analysis, the crew should be assumed properly trained, motivated and managed for their duties and suffering stress and fatigue only to the extent brought about by the environmental and operational conditions on the craft during its relatively short voyages. The analysis should in particular address the layout ergonomics of the system/operator interface.

Malfunctions due to software errors or inadequacies should also be taken into account as far as possible and determined both from the point of view of hardware and software design.

2.5 Failure effects (Local effects; End effects)

A failure effect is the consequence of a failure mode in terms of operation, function or status of a system. All failure effects need to be identified, evaluated and recorded. The consequences should also be described in terms of perturbation of the element's output.

It is necessary to differentiate between local failure effects and end failure effects. Local effects are those which affect the system under consideration. End effects are more generally related to the craft and should not be

limited to the system under analysis (e.g. failure of steering waterjet affects both propulsion and direction control systems).

An essential prerequisite of the FMEA is the definition and classification of the severity of the effects of failures of each system on the entire craft. On the basis of the general definitions of categories of severity of failure effects (Part A, 4.3), the meaning of catastrophic, hazardous, major or minor consequences of a failure should be specified for that particular system. Severity of failure refers basically to end effects (i.e. to the effects on the craft).

Examples of failure effects for components of different systems are given in Part C, 2.4 (Example 9).

2.6 Failure detection

The means and/or methods for detection of the failure mode should be described.

Failure modes which give rise to an identical manifestation should be analysed and listed.

The need for separate detection of failure of redundant elements during operation should be considered.

Means to detect failure, in particular in all those cases where corrective actions are foreseen and/or the severity of consequences which can be mitigated by prompt detection, should be indicated explicitly (e.g. indicators, alarms, manual detection, no detection) with the aim of evaluating the effectiveness of the corrective action.

Examples of detection means of the failures of components of different systems are given in Part C, 2.5 (Example 10).

2.7 Corrective actions

Corrective actions are those already foreseen by designers and/or normally used in the operational procedures to prevent or reduce the effects of failures. The severity of failures, has to be estimated by taking into account only these corrective actions.

Examples of corrective actions for the failures of components of different systems are given in Part C, 2.6 (Example 11).

Corrective measures are those actions which, as a result of the FMEA, have to be implemented to reduce the risk within acceptable limits and may include either redundancy or operational measures or a combination of the two. They must be mentioned in the "remarks" column of the FMEA and described in the document by explaining their effects in mitigating the risk. As a consequence of introducing a corrective measure, drawings, manuals and specifications relevant to the system involved must be modified as appropriate.

3. DETAILED ANALYSIS (2nd level)

A detailed analysis can be performed using the same worksheet of the 1st level analysis (annex 4 - Appendix 2 of the HSC Rules here annexed in Table 1). The end effect, in this case, is the effect of the failure mode on the higher system in the hierarchy (1st level).

In the 2nd level analysis, minor and major effects should be treated according to the same philosophy as used in level 1, i.e. if the item is not relevant to safety it can be discarded; if it is safety related, redundancy, corrective measures or probability concepts will have to be used.

4. RECOMMENDATIONS

The analysis report should include a section which summarises the results of the FMEA in a way which can be readily understood by all interested parties without expert knowledge in failure analysis techniques.

As a result of the FMEA, recommendations should be given about design modifications, operational procedures and other mitigation measures necessary to make acceptable those failure modes which have resulted unacceptable.

5. TEST PROGRAMME

5.1 General

Theoretical analysis results have to be verified by undertaking ship sea trials (annex 4 - 15 and annex 8 - 4 of the HSC Rules). The specification for these trials should be based on the results described in the FMEA report and should investigate the outcome of induced failures where appropriate.

Full-scale trials simulating the possible equipment failures have the aim of verifying:

- important working hypotheses, i.e. those initial assumptions which are the basis on which to affirm that the consequences (severity) of some failure modes are negligible or minor;
- corrective measures which reduce the consequences of a failure mode giving major or more severe effects to an acceptable level of severity (minor). In particular, it is important to check the effectiveness of a redundancy, alarms (kind and location), restricted operations and control sequence for automated systems.

For equipment where failure cannot be easily simulated on the craft, the results of other tests can be used to determine the effects and influences on the systems and craft. The trials should also include investigation into:

1) 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;
2) the existence and quality of operational documentation for the craft with particular regard to the pre-departure checklists. It is essential that these checks account for any unrevealed failure modes identified in the failure analysis; and
3) the effects of the main failure modes as prescribed in the theoretical analysis.

5.2 Additional tests to be carried out in the trials

As specified in annex 8 - 4.3 of the HSC Rules, the following tests need to be carried out in addition to those resulting from the theoretical analysis:

1) total loss of propulsion power
2) total loss of lift power (for ACV and SES)
3) total failure of control of one propulsion system
4) involuntary application of full propulsion thrust (positive or negative) on one system
5) failure of control of one directional control system
6) involuntary full deflection of one directional control system
7) failure of control of trim control system
8) (involuntary) full deflection of one trim control system element; and
9) total loss of electrical power
10) "Dead ship" test (The craft should be stopped and all main machinery shut down for sufficient time so that the craft's heading relative to wind and waves has stabilised. The purpose of the test is to establish craft motions and direction of laying to wind and waves. Therefore the test has to be carried out, on opportunity basis, under different wind and sea states.)

Based on the results of the FMEA, the above tests can be specified so as to better reflect the craft's characteristics and its functional redundancies.

As an example, for a category B craft having at least two completely separate engine rooms, test (1) can be carried out by simulating separately the complete loss of each engine room.

5.3 FMEA test programme

An FMEA test programme is to be agreed and enclosed with the FMEA report.

For each test, the programme needs to include the following information:

- test scope
- system, element, function, failure mode, failure cause, reference to worksheet, craft operating condition, severity of failure, probability of failure (as appropriate)
- description of failure simulation
- expected failure detection
- expected local failure effect (i.e. effects on the system)
- expected end effect on the craft
- expected corrective action.

It is recommended to include the above information in a checklist form to be used to report the test.

An example of the test checklist for a craft having 4 propulsion lines is shown in Table 2 hereto annexed.

TABLE 1

FMEA WORKSHEET

N°	Item description			Failure description		Failure effect		Failure	Corrective	Severity	Probabilit y	Remarks /
	Name	Id.	Function	Mode	Cause	Local	End	Detection	Action	of Failure	of Failure	Comments

TABLE 2

Example of FMEA trial test sheet (four propulsion line craft)

FMEA TEST PROGRAMME SHEET							NO.	
CRAFT					DATE		TIME	
DISPLACEMENT		SPEED		OPERATIONAL MODE		SEA STATE		
TEST SCOPE								

SYSTEM		EQUIPMENT	
FUNCTION		FAILURE MODE	
FAILURE CAUSE		FMEA REF.	
FAILURE SIMULATION			

FAILURE DETECTION

	PORT WING PROPULSION LINE	PORT INNER PROPULSION LINE	STBD INNER PROPULSION LINE	STBD WING PROPULSION LINE	MONITORING AND ALARM SYSTEM
EXPECTED					
OBSERVED					

LOCAL FAILURE EFFECTS

	PORT WING PROPULSION LINE	PORT INNER PROPULSION LINE	STBD INNER PROPULSION LINE	STBD WING PROPULSION LINE	OTHER
EXPECTED					
OBSERVED					

BACK-UP SYSTEMS, CORRECTIVE ACTIONS

	PORT WING PROPULSION LINE	PORT INNER PROPULSION LINE	STBD INNER PROPULSION LINE	STBD WING PROPULSION LINE	OTHER
EXPECTED					
OBSERVED					

PROBABILITY	END EFFECTS ON THE CRAFT	SEVERITY
EXPECTED	EXPECTED	
OBSERVED	OBSERVED	

REMARKS	

PART C - EXAMPLES

1. EXAMPLES OF THE INFORMATION REQUIRED

1.1 Example 1: Description of the craft (see Part B, 1.2)

For the purposes of this example 1 and of all the following examples, a passenger ro-ro high speed craft, monohull, designated for short international voyages will be considered.

In the following table the **main characteristics** of the craft are shown:

Length overall	..... m
Length between pp	..... m
Max. breadth	..... m
Max. dead-weight capacity	..... t
Trial DWT	..... t
Depth	..... m
Displacement with its DWT	..... t
Corresponding draught	..... m
Payload capacity	n° of passengers, cars, coaches, ...
Propulsion power installed	..... kW
Electric power installed	..... kW
Average fuel consumption	..... t/h
Service speed	..... knots

Narrative description of the craft

The craft is provided with two passenger decks and two car decks.

The car embarking/disembarking operations are carried out through one stern vehicle ramp located in way of the upper car deck. A central ramp provides access to the lower car deck. The car decks have the capacity of ..... private cars. Alternatively ..... coaches can be accommodated on the upper car deck; in such a case the craft is able to carry ..... coaches and ..... private cars.

The passenger embarking/disembarking operations are carried out through two aft fire-resistant trunks (port and stbd side) and a fore truck (also fire-resistant) between the upper car deck and the main passenger deck. An internal stairway leads from the main passenger deck to the upper passenger deck.

The machinery is fitted in the extreme aft part of the ship and is subdivided into 3 watertight compartments, each including a complete shaft line: aft port engine room, aft starboard engine room, and fore engine room (booster and main generator room). Access to each engine room is from the upper garage deck. The three compartments are connected to each other by watertight doors motorised from the wheel-house. Each compartment includes all the equipment relevant to one shaft line. Each propulsion line can be considered fully independent from the others, having independent auxiliary systems and control devices, in order to guarantee the full availability of the ship also in case of the loss of one engine room. A wing steering/reversing waterjet powered by one diesel engine is fitted in each aft engine room. Two other diesel engines are located in the fore engine room and power one booster waterjet having thrust function only. One bow-thruster is provided for better manoeuvring.

The fore engine room also includes two main generating sets and the main switchboard. The auxiliary generator room, including the auxiliary generating set and the emergency switchboard is located at the fore end of the lower garage. The auxiliary generating set is connected to the emergency switchboard and is provided with independent auxiliary systems, monitoring and control devices.

The wheel-house, located in superelevated position on the upper passenger deck, contains the bridge console, divided into three sections including; all the monitoring and control devices for the propulsion system, hull plants and generating sets; the control device for handling of the craft; and navigation and radio-communication instruments.

A **general arrangement plan showing the main systems** of the craft (such as propulsion plant, electrical system, stabilisation system, craft control systems, craft users essential for safety in an emergency) should be enclosed with the craft description (e.g. using the craft drawings).

A **block diagram representing the craft's main systems** and the relationships between such systems is shown in figure 1.

In the following tables the **operative profile of the craft** during the year is shown:

Period	months	days	voyages/day	number of voyages	work T(h)
high season					
middle season					
low season					
maintenance					

operative days per year	
voyages per year(total number)	
average voyages / day	
total working time per year(h)	

1.2 Example 2: Narrative description of one system (see Part B, 1.3)

Stabilisation system: installed for passenger comfort to continuously and automatically counteract the roll motion imparted to the ship by sea movement. It basically consists of two different parts: hydrodynamic equipment and electronic control devices. The hydrodynamic equipment includes all the machinery which receives and carries out the commands of the solid-state electronic control system.

Description of system structure

As illustrated in the system block diagram (Example 4), the system is composed of a couple of retractable fin stabilisers, starboard and port side. The fins are fitted with two hydraulic cylinders controlling respectively the position (in or out) and the oscillation of the fins (**fin rig-in cylinder** and **fin oscillation cylinder**) and with a **lock device** which is fitted to lock the fin in the rigged-in position. Each fin is also equipped with an **electro-hydraulic group**. The control system, which perceives and works out ship roll motion data and transmits relevant commands to the hydrodynamic equipment, consists of a **bridge control panel**, which allows the remote control and monitoring of the system, a **main control unit,** which is located in the stabilising room on the ship lower deck and perceives the rolling movements of the ship, calculates the correct righting moment and sends corresponding signals to the local control units, and two independent **local control units**, each situated in proximity of the relevant fin, which is fitted to control the position of each fin.

The different system elements are listed below:

* Fin oscillation cylinder (FOC)
* Fin rig-in cylinder (FRC)
* Fin lock device (FLD)
* Hydraulic circuit (HC)
* Oil tank (OT)
* Oil Heat exchanger (OHE)
* Local control unit (LCU)
* Main control unit (MCU)
* Bridge control panel (BCP)

A brief description of the characteristics, functions and operating modes is given for each or the above elements; this can be either narrative (example following for the main control unit) or tabular (Example 3). In the following an example relevant to the **main control unit**: is shown:

> The main control unit houses the lift computer assembly, the 400 Hz static power supply, a control and monitor panel and the roll motion sensor unit.

Its function is to sense the ship's roll motions, to compute the lift required to counteract the ship's roll, to provide control and to provide monitoring facilities for crew use.

An alarm circuit is incorporated to give warning of certain abnormal conditions, and test points are provided for fault findings and maintenance purposes.

The logical connections between elements, like the inputs and outputs of the system and its elements, are shown in the block diagram in the following Example 4.

The system contains the following auxiliaries (as also indicated in the block diagram):

- oil tank, one for each fin oscillation cylinder, to keep the fin casing in which each fin shaft is contained under pressure;
- oil heat exchanger, one for each hydraulic circuit, to cool the oil with sea water supplied by a single pump driven by the right propulsion diesel engine located in the fore engine room.

The system is connected to the electrical system and the propulsion system: the main control unit and the local control units are fed by the electrical system, and the sea water pump for the oil heat exchanger is driven by the right propulsion diesel engine located in the fore engine room.

Within the hydraulic circuit a back-up electrical pump is installed to intervene in case of failure of the main pump. The redundant pump is fed by the emergency switchboard so as to be able to start for emergency manoeuvres.

Description of system operation and control

The stabilisation system does not operate when the craft is manoeuvring alongside. In normal operating conditions the system is automatically driven by the main control unit. In emergency conditions, the system can be manually operated to rig fins in.

Since the system is installed for passenger comfort only, it does not have direct effects on craft safety. For this reason, unavailability of the system is not to be considered as an end effect on the craft because it is a negligible effect. The only case to be considered is when a fin is blocked in the out position with an angle different from zero. This event produces major consequences as it may affect craft manoeuvrability.

The system becomes active when the prescribed average levels of roll motions are exceeded. In these conditions the system operates continuously.

When a fin is blocked in the out position, corrective action, to ensure manoeuvrability of the craft, is to be carried out as soon as possible (within minutes), particularly in congested waters.

In normal conditions, interfaces and interactions of the system with operators are realised through the bridge control panel.

Environmental conditions which guarantee the normal operating conditions of the system

No specific environmental conditions affect the performance of the system.

List of reference design drawings and documents

More detailed information on the main sub-systems and equipment of the stabilisation system can be obtained from drawings no. ..... and ..... and from the craft operating manual and maintenance and servicing manual.

1.3 Example 3: Sheet for one element of the system (see Part B, 1.3)

CRAFT: passenger ro-ro HSC FMEA level: 1	
SYSTEM NAME	Stabilisation system
ELEMENT NAME	Main Control Unit
REFERENCE	MCU - Drawing Ref..... - Block diagram: .....
FUNCTION	To sense the ship's roll motions, to compute the lift required to counteract the ship's roll, to provide control and to provide monitoring facilities for crew use.
CHARACTERISTICS	The main control unit houses the lift computer assembly, the 400 Hz static power supply, a control and monitor panel and the roll motion sensor unit. An alarm circuit is incorporated to give warning of certain abnormal conditions, and test points are provided for fault findings and maintenance purposes.
OPERATING MODES: • NORMAL • ABNORMAL	Main control unit working correctly: all functions available. When the main control unit loses its functions due to loss of electrical power, hardware failure or software failure
INPUT/OUTPUT	Input: electrical signals from bridge control panel (control signal), roll motion sensor unit (signal coming from sensor measuring craft's motions and angular speeds), local control units (feedback signal from a fin angle transmitter to be compared with its output signal); and electrical power from the electrical system. Output: electrical signals to the local control units (control signals) and to the bridge control panel (monitoring signals)
RELATED SYSTEMS	Electrical system
REDUNDANCY	None
CORRECTIVE ACTIONS	Emergency shutdown procedures; rig-in both fins under local control

1.4 Example 4: Block diagram of one system (see Part B, 1.4)

In figure 2 the block diagram of the stabilisation system is given. Each element into which the system is broken down is identified by a code (e.g. main control unit = MCU).

Functional relationships among the system elements are indicated, as well as inputs and outputs to/from the blocks, including those to/from other systems (e.g. mechanical power (MP), electrical power (EP), hydraulic power (HP) and electrical signal (ES)).

1.5 Example 5: Identification of the boundaries of one system (see Part B, 1.5)

The boundaries of the stabilisation system are shown in the block diagram (Example 4). In the following an explanation why certain components have not been included in the block diagram is given. It is to be noted that no such explanation is to be provided in the FMEA report unless it is essential to understand the block diagram itself.

The stabilisation system is considered in its function to continuously and automatically counteract the roll motion imparted to the ship by sea movement for passenger comfort.

In view of this function of the system, the identified elements considered part of the system are the two stabilisation fins and their relevant physical and electronic controls as listed below:

* Fin oscillation cylinder (FOC)
* Fin rig-in cylinder (FRC)
* Fin lock device (FLD)
* Hydraulic circuit (HC)
* Oil tank (OT)
* Oil heat exchanger (OHE)
* Local control unit (LCU)
* Main control unit (MCU)
* Bridge control panel (BCP)

The boundaries are such that, although the system is connected to the electrical system (which feeds the main control unit and the local control units) and the propulsion system (which drives the pump providing sea water to the heat exchanger), the main switchboard, the 24V distribution panel, the right propulsion diesel engine in the fore engine room, etc. are not considered elements of the system.

This means that, for example, the various failures of the main switchboard are not considered among the failure modes of this system (because the main switchboard has not been considered a component of the system); it appears in the analysis only as failure cause of the Main Control Unit (loss of electrical power).

It therefore results clear that the definition of the system boundaries limits the number of failure modes to be considered and implies the inclusion of "loss of inputs from other systems" among the potential causes of failures of a certain element.

2. EXAMPLES OF FUNCTIONAL FAILURE ANALYSIS OF IMPORTANT SYSTEMS (1ST LEVEL)

2.1 Example 6: Worksheet (see Part B, 2.2)

An example of a worksheet of the stabilisation system as defined in the above examples is shown in appendix 1.

2.2 Example 7: Failure modes (see Part B, 2.3)

A list of failure modes of the hydraulic circuit of the stabilisation system is given in the following. Since the failure mode is the loss of function of the system, the function of the component is also indicated:

Functions	Failure modes
to supply hydraulic power to the fin	complete loss of output
	loss of output to fin oscillation cylinder
	loss of output to fin positioning cylinder
	loss of output to fin lock device
	serious oil leakage

A list of failure modes of the steering water jet of the machinery and directional system is given in the following. The various functions of the steering water jet are also indicated and, for each one, the relevant failure modes:

Functions	Failure modes
to supply thrust	complete loss of output
	rapid change to minimum output
to allow craft's directional control and stoppage during navigation	complete loss of output
	rapid change to minimum output
to allow craft's stoppage during navigation	reversing bucket fails to operate
to allow craft's directional control during navigation	steering nozzle failure

A list of failure modes of the emergency switchboard of the electrical system is given in the following. The various functions of the emergency switchboard are also indicated and, for each, the relevant failure modes:

Functions	Failure modes
to distribute electrical power to various craft users during normal conditions	loss of tension
to distribute 220V electrical power to certain craft users during normal conditions	loss of 220V power supply

Note: in this example, a small number of non-vital users are fed only by the emergency switchboard in normal operating conditions. The failures of the emergency switchboard (e.g. loss of tension) in its function of distributing electrical power to craft users during emergency conditions, that is when a failure of the main switchboard has already occurred, are not to be considered because the analysis is based on a single failure concept (see Part A, 4.1).

2.3 Example 8: Failure causes (see Part B, 2.4)

A list of failure causes of the hydraulic circuit of the stabilisation system is given in the following. Since the failure cause is associated with a failure mode, the failure modes of the component are also indicated:

Failure modes	Failure causes
complete loss of output	hydraulic oil tank empty pump failures loss of electrical power
loss of output to fin oscillation cylinder	failure of distributor to fin oscillation cylinder
loss of output to fin positioning cylinder	failure of distributor to fin positioning cylinder
loss of output to fin lock device	failure of distributor to fin lock device
serious oil leakage	seal failures

A list of failure causes of the steering water jet of the machinery and directional system is given in the following. The various failure modes of the steering water jet are also indicated and, for each, the relevant failure causes:

Failure modes	Failure causes
complete loss of output	rotor breaking off complete loss of propulsion line rotor blockage complete obstruction of aspiration duct
rapid change to minimum output	partial obstruction of aspiration duct
reversing bucket fails to operate	blockage of reversing bucket
steering nozzle failure	blockage of steering nozzle in actual position

A list of failure causes of the emergency switchboard of the electrical system is given in the following. The various failure modes of the emergency switchboard are also indicated and, for each, the relevant failure causes:

Failure modes	Failure causes
loss of tension	loss of electrical power supply from the main switchboard loss of electrical power supply from emergency diesel generator short circuit
loss of 220V power supply	220V bus bar short circuit transformer failure

2.4 Example 9: Failure effects (Local effects; End effects) (see Part B, 2.5)

A list of failure effects (both local and end) of the hydraulic circuit of the stabilisation system is given in the following. Since the failure effect is associated with a failure mode, the failure modes of the component are also indicated:

Failure modes	Local Failure effects	End Failure effects
complete loss of output	low pressure no hydraulic pressure	loss of stabilisation system loss of stabilisation system
loss of output to fin oscillation cylinder	loss of fin oscillation	manoeuvrability problems
loss of output to fin positioning cylinder	fin blocked in actual position	manoeuvrability problems
loss of output to fin lock device	fin blocked in IN position	loss of stabilisation system
serious oil leakage	no hydraulic pressure	loss of stabilisation system

A list of failure effects (both local and end) of the steering water jet of the machinery and directional system is given in the following. The various failure modes of the steering water jet are also indicated and, for each, the relevant failure effects:

Failure modes	Local Failure effects	End Failure effects
complete loss of output	complete loss of propulsion line	small reduction (25%) of craft's propulsion capabilities; reduction of craft's directional control and stoppage capabilities
rapid change to minimum output	reduction of water jet output	negligible reduction of craft's propulsion capabilities; negligible reduction of craft's directional control and stoppage capabilities
reversing bucket fails to operate	unsuccessful reversal of jet's direction	increased craft trackreach
steering nozzle failure	loss of directional control	reduction of craft's directional control

A list of failure effects (both local and end) of the emergency switchboard of the electrical system is given in the following. The various failure modes of the emergency switchboard are also indicated and, for each, the relevant failure effects:

Failure modes	Local Failure effects	End Failure effects
loss of tension (during normal conditions)	total loss of normal power supply to all craft users directly connected to emergency switchboard	total loss of power supply to all craft users fed by the emergency switchboard only
loss of 220V power supply	loss of tension in the 220V bus-bar of emergency switchboard	loss of electrical power supply to all craft users directly connected to the 220V bus-bar of the emergency switchboard

2.5 Example 10: Failure detection (see Part B, 2.6)

A list of detection means for the failures of the hydraulic circuit of the stabilisation system is given in the following:

Failure modes	Failure detection means
complete loss of output	low hydraulic oil pressure indicator
loss of output to fin oscillation cylinder	fin angle indicator
loss of output to fin positioning cylinder	fin IN/OUT indicators
loss of output to fin lock device	fin IN indicator
serious oil leakage	low hydraulic oil pressure indicator

A list of detection means for the failures of the steering water jet of the machinery and directional system is given in the following:

Failure modes	Failure detection means
complete loss of output	overspeed alarm (total obstruction of asp. duct) loss of thrust control alarm (rotor blockage) indication of low engine power output (partial obstruction of asp. duct)
rapid change to minimum output	indication of low engine power output
reversing bucket fails to operate	reversing control failure alarm
steering nozzle failure	steering control failure alarm

A list of detection means for the failures of the emergency switchboard of the electrical system is given in the following:

Failure modes	Failure detection means
loss of tension during normal conditions	ship monitoring system: loss of normal electrical supply alarm main switchboard: loss of tension alarm emergency switchboard: loss of tension alarm generator sets: main failure alarm various users: loss of electrical power alarm
loss of 220V power supply	main switchboard: loss of 220V tension alarm various 220V users: loss of electrical power alarm

2.6 Example 11: Corrective actions (see Part B, 2.7)

A list of corrective actions for the failures of the hydraulic circuit of the stabilisation system is given in the following:

Failure modes	Corrective actions
complete loss of output	emergency shut-down procedures; rig IN both fins under local control; start emergency pump to set fin angle to zero and use manual pump to rig IN the fin
loss of output to fin oscillation cylinder	emergency shut-down procedures; start emergency pump to set fin angle to zero and use manual pump to rig IN the fin; rig IN other fin under local control
loss of output to fin positioning cylinder	emergency shut-down procedures; start emergency pump to set fin angle to zero and use manual pump to rig IN the fin; rig IN other fin under local control
loss of output to fin lock device	emergency shut-down procedures; rig IN other fin under local control
serious oil leakage	emergency shut-down procedures; rig IN both fins under local control

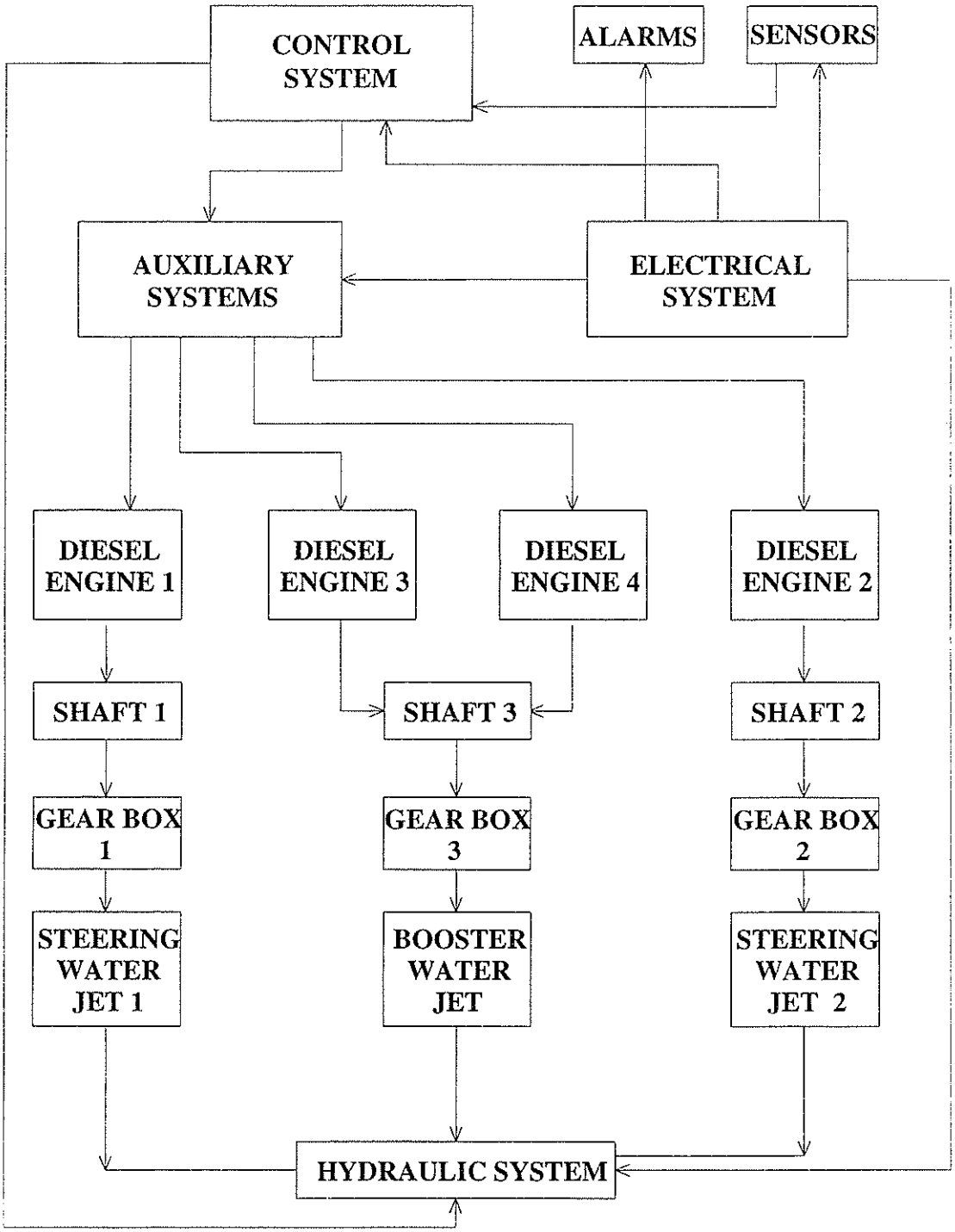
A list of corrective actions for the failures of the steering water jet of the machinery and directional system is given in the following:

Failure modes	Corrective actions
complete loss of output	engine shut down deactivation of propulsion line local inspection
rapid change to minimum output	local inspection
reversing bucket fails to operate	engine speed reduction to idle; deactivation of propulsion line
steering nozzle failure	engine speed reduction to idle; deactivation of propulsion line

A list of corrective actions for the failures of the emergency switchboard of the electrical system is given in the following:

Failure modes	Corrective actions
loss of tension during normal conditions	release of emergency switchboard from main switchboard; start-up and connection of emergency diesel generator set to the emergency switchboard; starting of blackout relevant emergency procedures; local inspection; emergency switchboard short circuit protection devices (if the failure cause is short circuit)
loss of 220V power supply	use static converter battery to supply certain users; local inspection

FIGURE 1


CONTROL SYSTEM
ALARMS
SENSORS
AUXILIARY SYSTEMS
ELECTRICAL SYSTEM
DIESEL ENGINE 1
DIESEL ENGINE 3
DIESEL ENGINE 4
DIESEL ENGINE 2
SHAFT 1
SHAFT 3
SHAFT 2
GEAR BOX 1
GEAR BOX 3
GEAR BOX 2
STEERING WATER JET 1
BOOSTER WATER JET
STEERING WATER JET 2
HYDRAULIC SYSTEM

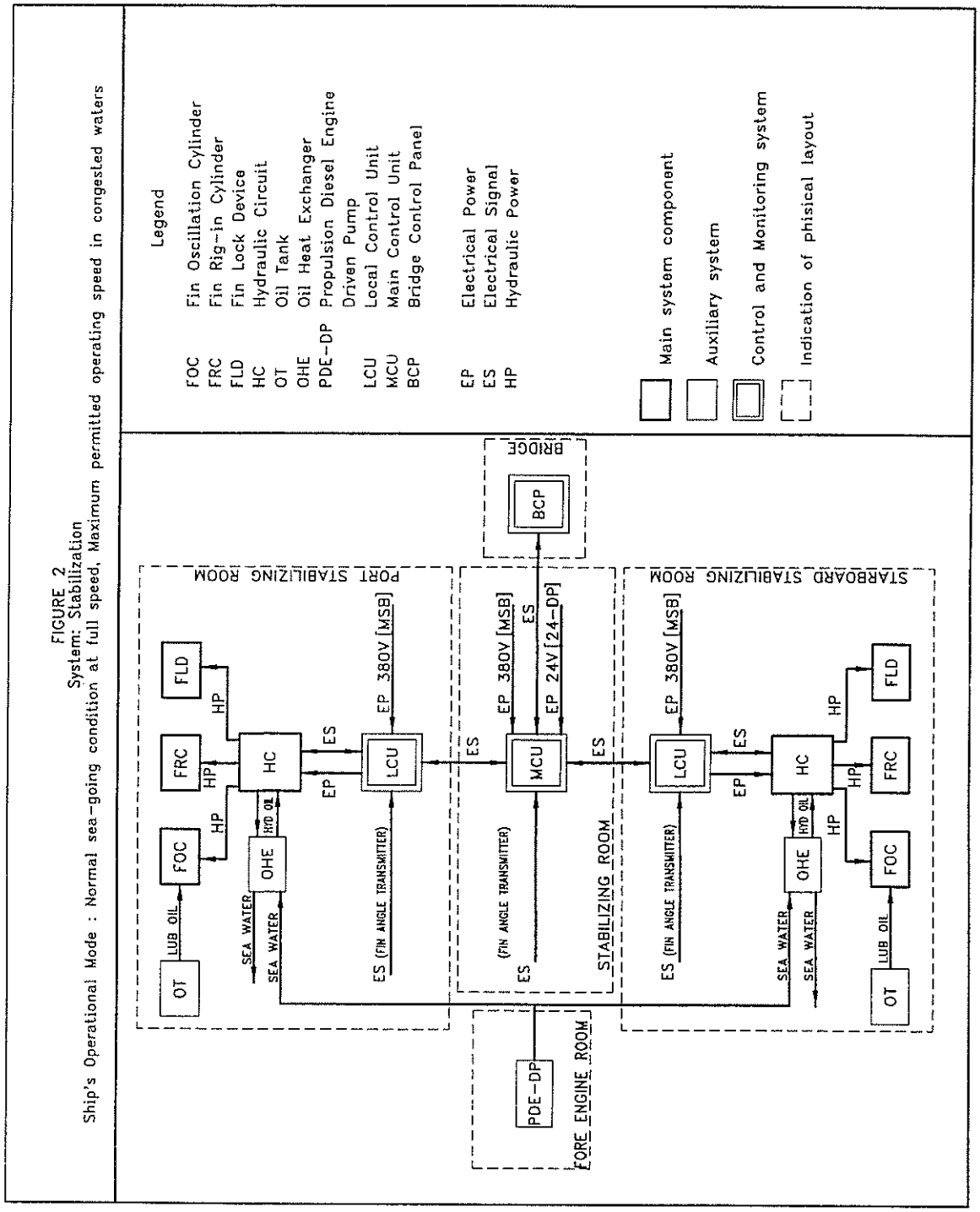


FIGURE 2
System: Stabilization
Ship's Operational Mode : Normal sea-going condition at full speed, Maximum permitted operating speed in congested waters

APPENDIX 1

Stabilisation system

Ship's operational mode: normal sea-going conditions at full speed
maximum permitted operating speed in congested waters

N°	Item description			Failure description		Failure effect		Failure	Corrective	Severity	Probability	Remarks /
	Name	Id.	Function	Mode	Cause	Local	End	Detection	Action	of Failure	of Failure	Comments
23.1	Hydraulic Circuit	HC	To supply hydraulic power to the fin	Total loss of output	Pump failures	No hydraulic pressure	Loss of stabilisation system	Low hydraulic oil pressure indicator	Emergency shutdown procedures. Start emergency e/pump to set fin angle to zero and use manual pump to rig-IN the fin Rig IN other fin under local control	Minor		It is recommended to periodically check e/pump and manual pump of each hydraulic circuit
23.2	Hydraulic Circuit	HC	To supply hydraulic power to the fin	Loss of output top fin lock device	Relevant distributor failure	Fin blocked in IN position	Loss of stabilisation system	Fin IN indicator	Emergency shutdown procedures Rig IN other fin under local control	Minor		