Annex 4
Procedures for Failure Mode and Effects Analysis

1 Introduction

1.1 In the case of traditional craft, it has been possible to specify certain aspects of design or construction in some level of detail, in a way which was consistent with some level of risk which had over the years been intuitively accepted without having to be defined.

1.2 With the development of large high speed craft, this required experience has not been widely available. However, with the now broad acceptance of the probabilistic approach to safety assessments within industry as a whole, it is proposed that an analysis of failure performance may be used to assist in the assessment of the safety of operation of high speed craft.

1.3 A practical, realistic and documented assessment of the failure characteristics of the craft and its component systems should be undertaken with the aim of defining and studying the important failure conditions that may exist.

1.4 This annex describes a failure mode and effects analysis (FMEA) and gives guidance as to how it may be applied by:

.1 explaining basic principles;

.2 providing the procedural steps necessary to perform an analysis;

.3 identifying appropriate terms, assumptions, measures and failure modes; and

.4 providing examples of the necessary worksheets.

1.5 FMEA for high speed craft is based on a single failure concept under which each system at various levels of a system's functional hierarchy is assumed to fail by one probable cause at a time. The effects of the postulated failure are analysed and classified according to their severity. Such effects may include secondary failures (or multiple failures) at other level(s). Any failure mode which may cause a catastrophic effect to the craft should be guarded against by system or equipment redundancy unless the probability of such failure is extremely improbable (refer to section 13). For failure modes causing hazardous effects corrective measures may be accepted in lieu. A test programme should be drawn to confirm the conclusions of FMEA.

1.6 Whilst 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.

2 Objectives

2.1 The primary objective of FMEA is to provide a comprehensive, systematic and documented investigation which establishes the important failure conditions of the craft and assesses their significance with regard to the safety of the craft, its occupants and the environment.

2.2 The main aims of undertaking the analysis are to:

.1 provide the Administration with the results of a study into the craft's failure characteristics so as to assist in an assessment of the levels of safety proposed for the craft's operation;

.2 provide craft operators with data to generate comprehensive training, operational and maintenance programmes and documentation; and

3 provide craft and system designers with data to audit their proposed designs.

3 Scope of application

3.1 FMEA should be conducted for each high speed craft, before its entry into service, in respect of the systems as required under the provisions of 5.2, 9.1.10, 12.1.1 and 16.2.6 of this Code.

3.2 For craft of the same design and having the same equipment, one FMEA on the lead craft will be sufficient, but each of the craft should be subject to the same FMEA conclusion trials.

4 System failure mode and effects analysis

4.1 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 craft's important systems. In this way only systems which fail the functional failure analysis need to be investigated by a more detailed FMEA.

4.2 When conducting a system FMEA the following typical operational modes within the normal design environmental conditions of the craft should be considered:

.1 normal seagoing conditions at full speed;
.2 maximum permitted operating speed in congested waters; and
.3 manoeuvring alongside.

4.3 The functional interdependence of these systems should also be described in either block diagrams or fault tree diagrams or in a narrative format to enable the failure effects to be understood. As far as applicable, each of the systems to be analysed is assumed to fail in the following failure modes:

.1 complete loss of function;

.2 rapid change to maximum or minimum output;

.3 uncontrolled or varying output;

.4 premature operation;

.5 failure to operate at a prescribed time; and

.6 failure to cease operation at a prescribed time.

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

4.4 If a system can fail without any hazardous or catastrophic effect, there is no need to conduct a detailed FMEA into the system architecture. For systems whose individual failure can cause hazardous or catastrophic effects and where a redundant system is not provided, a detailed FMEA as described in the following paragraphs should be followed. Results of the system functional failure analysis should be documented and confirmed by a practical test programme drawn up from the analysis.

4.5 Where a system, the failure of which may cause a hazardous or catastrophic effect, is provided with a redundant system, a detailed FMEA may not be required provided that:

.1 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 in 4.2 without hazarding the craft;

.2 the redundant system is completely independent from 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. Common system element may be acceptable if the probability of failure complies with section 13; and

.3 the redundant system may share the same power source as the system. In such case an alternative power source should be readily available with regard to the requirement of .1.

The probability and effects of operator error to bring in the redundant system should also be considered.

5 Equipment failure mode and effects analysis

The systems to be subject to a more detailed FMEA investigation at this stage should include all those that have failed the system FMEA and may include those that have a very important influence on the safety of the craft and its occupants and which require an investigation at a deeper level than that undertaken in the system functional failure analysis. These systems are often those which have been specifically designed or adapted for the craft, such as the craft's electrical and hydraulic systems.

6 Procedures

The following steps are necessary to perform FMEA:

.1 to define the system to be analysed;

.2 to illustrate the interrelationships of functional elements of the system by means of block diagrams;

.3 to identify all potential failure modes and their causes;

.4 to evaluate the effects on the system of each failure mode;

.5 to identify failure detection methods;

.6 to identify corrective measures for failure modes;

.7 to assess the probability of failures causing hazardous or catastrophic effects, where applicable:

.8 to document the analysis;

.9 to develop a test programme;

.10 to prepare FMEA report.

7 System definition

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. A narrative description of the system and its functional requirements should be drawn up including the following information:

.1 general description of system operation and structure;

.2 functional relationship among the system elements;

.3 acceptable functional performance limits of the system and its constituent elements in each of the typical operational modes: and

.4 system constraints.

8 Development of system block diagrams

8.1 The next step is to develop block diagram(s) showing the functional flow sequence of the system, both for technical understanding of the functions and operation of the system, and for the subsequent analysis. As a minimum the block diagram should contain:

.1 breakdown of the system into major sub-systems or equipment;

.2 all appropriate labelled inputs and outputs and identification numbers by which each sub-system is consistently referenced; and

.3 all redundancies, alternative signal paths and other engineering features which provide "fail-safe" measures. An example of a system block diagram is given at appendix 1

8.2 It may be necessary to have a different set of block diagrams prepared for each operational mode.

9 Identification of failure modes, causes and effects

9.1 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 table 1. The failure modes listed in table 1 can describe 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).

9.2 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 become a failure cause of the steering gear system's failure mode "loss of output"(29).

9.3 Each system should be considered in a top-down approach, starting from the system's functional output, and failure should 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 should be identified.

9.4 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 should be shown to be immediately effective or brought on line with negligible time lag. In addition, if the sequence is:
"failure-alarm-operator action - start of back up - back up in service", the effects of delay should be considered.

10 Failure effects

10.1 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 system level. In certain instances, there may not be a local effect beyond the failure mode itself.

10.2 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:

.1 catastrophic;

.2 hazardous;

.3 major; and

.4 minor.

The definitions of these four categories of failure effects are given in 2.3 of annex 3 of this Code.

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

11 Failure detection

11.1 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 should be identified.

11.2 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 should 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.

12 Corrective measures

12.1 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 a system element or equipment, should also be identified and evaluated.

12.2 Provisions which are features of the design at any system level 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, should be described. 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; and

.3 alternative modes of operation.

12.3 Provisions which require operator action to circumvent or mitigate the effects of the postulated failure should be described. The possibility and effect of operator error should be

considered, if the corrective action or the initiation of the redundancy requires operator input, when evaluating the means to eliminate the local failure effects.

12.4 It should be noted that corrective responses acceptable in one operational mode may not be acceptable at another, e.g., a redundant system element with considerable time lag to be brought into line, while meeting the operational mode "normal seagoing conditions at full speed" may result in a catastrophic effect in another operational mode, e.g., "maximum permitted operating speed in congested water".

13 Use of probability concept

13.1 If corrective measures or redundancy as described in preceding paragraphs are not provided for any failure, as an alternative the probability of occurrence of such failure should meet the following criteria of acceptance:

.1 a failure mode which results in a catastrophic effect should be assessed to be extremely improbable;

.2 a failure mode assessed as extremely remote should not result in worse than hazardous effects;

.3 a failure mode assessed as either frequent or reasonably probable should not result in worse than minor effects.

13.2 Numerical values for various levels of probabilities are laid down in section 3 of annex 3 of this Code. In areas where there is no data from craft to determine the level of probabilities of failure other sources can be used such as:

.1 workshop test, or

.2 history of reliability used in other areas under similar operating conditions, or

.3 mathematical model if applicable.

14 Documentation

14.1 It is helpful to perform FMEA on worksheet(s) as shown in appendix 2.

14.2 The worksheets(s) should be organised to first display the highest system level and then proceed down through decreasing system levels.

15 Test programme

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

.1 major or more severe effects;

.2 restricted operations; and

.3 any other corrective action.

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.

15.2 The trials should also include investigations 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 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; and

.3 the effects of the main failure modes as prescribed in the theoretical analysis.

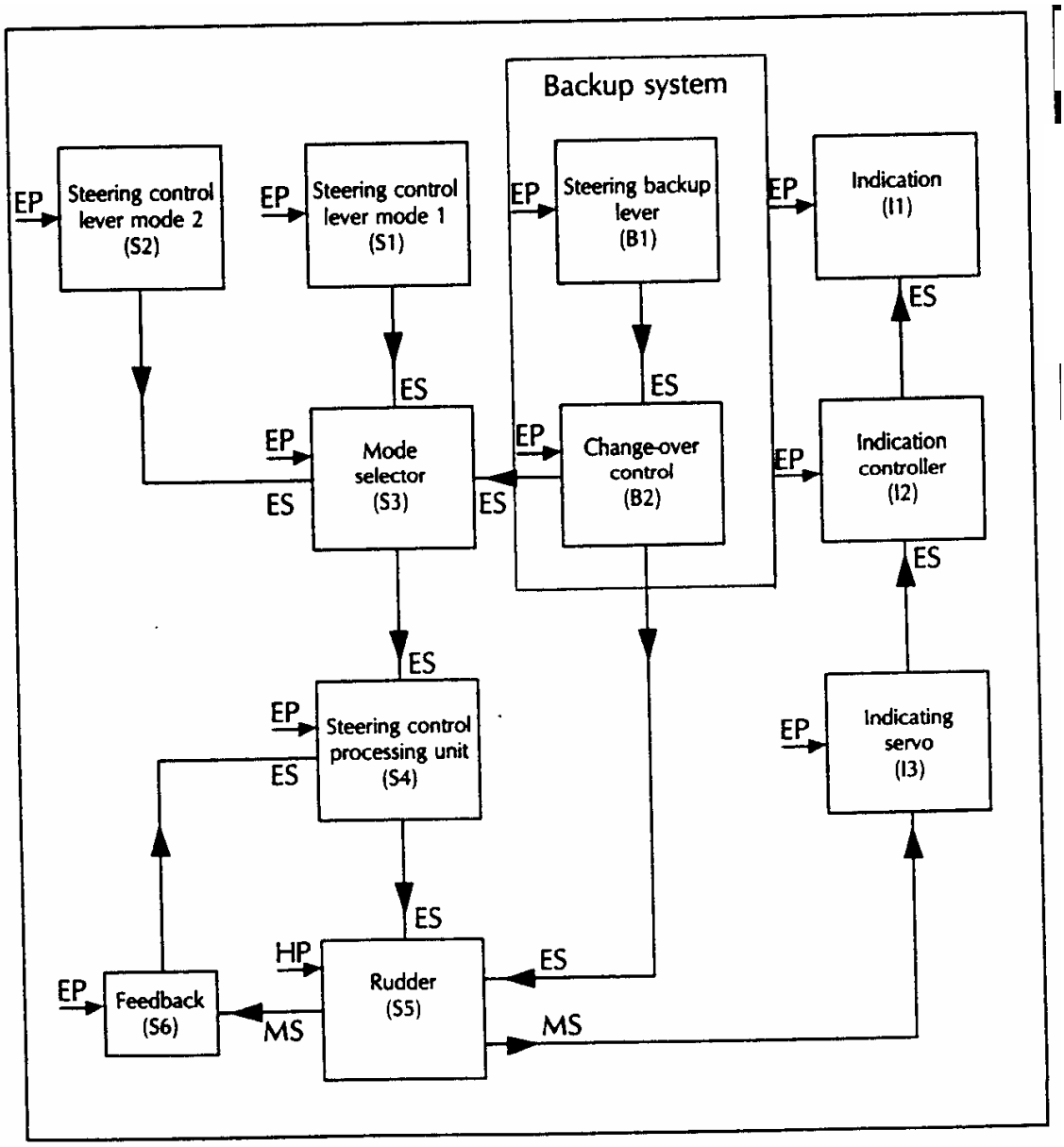
15.3 The FMEA tests on board should be conducted in conjunction with provisions specified in 5.3, 16.4 and 17.4 of this Code, before the craft enters into service.

16 FMEA Report

The FMEA report should 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 should be included, where appropriate. The report should contain a summary of conclusions and recommendations for each of the systems analysed in the system failure analysis and the equipment failure analysis. It should also 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 should contain the test programme, reference any other test reports and the FMEA trials.

Appendix 1
Example of a system block diagram

Steering Control System
Date.....
Analyst.....



Where :

EP - electrical power
HP - hydraulic power
ES - electrical signal
MS - mechanical signal

Table 1
Example of a set of failure modes

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

Refer to IEC Publication: IEC 812 (1985), Analysis techniques for system reliability - procedure for failure mode and effects analysis (FMEA).

Appendix a

FMEA worksheet

Name of system..... References.....
Mode of operation..... System block diagrams.....
Sheet No..... .....
Date..... .....
Name of analyst..... Drawings.....

Equipment name or number	Function	Ident. No.	Failure mode	Failure cause	Failure effect _____ Local effect End effect	Failure detection	Corrective action	Severity of failure effect	Probability of failure (If applicable)	Remarks	