CHAPTER 33

R&M FAILURE MODES, EFFECTS (AND CRITICALITY) ANALYSES (FMEA/FMECA)

CONTENTS

1. INTRODUCTION

1.1 A Failure Modes and Effects Analysis (FMEA) is a method of establishing the effect of failure within systems or processes; when applied to processes it is called a Process FMEA. This analysis can be performed at any level of an individual assembly. This may also be done together with a criticality analysis (CA). The combined exercise is then called a Failure Modes, Effects and Criticality Analysis (FMECA).

NOTE: The term FMECA shall be used throughout this guidance unless there is the need to clarify the attributes of FMEA or FMECA separately.

1.2 FMECA is a design audit activity and should be carried out jointly by reliability engineers and design staff; and other interested parties.

1.3 The analysis should address hardware, firmware, software and human elements of the product/process.

1.4 The purpose of a criticality analysis is to rank each potential failure mode identified in the FMEA according to the combined influence of the probability of occurrence and the severity of the failure effect.

1.5 Although the technique is inherently simple, its application has been misunderstood and frequently misinterpreted and consequently many organisations have failed to gain sufficient benefits that could resulted if it was to be applied properly.

2. SCOPE

The following attributes of the FMECA are discussed in this chapter:

a) Benefits and limitations.

b) Uses.

c) Procedure.

d) Design action.

e) FMECA report.

f) Maintainability aspects of FMECA.

g) Use of software.

3. BENEFITS AND LIMITATIONS

3.1 The benefits to be gained from performing an FMECA are that:

a) It provides designers with an understanding of the factors which influence the reliability of a system.

b) It identifies all failure modes which have a significant effect on system reliability and so provides an objective basis for deciding priorities for corrective design action.

c) It provides designers with information on the affects of component and subassembly failures which can be used to design fault detection and isolation methodologies.

3.2 The limitations of performing an FMECA are:

a) It can only be used to analyse single point failures.

b) It can be time consuming, but, if done properly, it is cost effective and its benefits outweigh the limitations.

4. USE

4.1 FMEA's are an essential part of the design process. They should be integrated with all other design activities and not simply treated as an off-line task. Outputs from FMEA's should be used as inputs to design reviews or reliability design evaluations so as to:

a) Identify and assess high risk items and areas.

b) Identify areas for specific attention during production.

c) Identify where special manufacturing processes, inspection, test or maintenance requirements may be required.

d) Establish if there are any operational constraints imposed by the design.

e) Identify failure modes which damage other components such that steps can be taken to protect them.

4.2 Products/processes can only be improved by corrective action to remove or reduce failure modes identified by FMECA.

4.3 An FMEA or an FMECA can be performed either qualitatively or quantitatively. A qualitative analysis is appropriate in the earlier stages of a project and the quantitative analysis is more appropriate in the later stages when more data is available.

4.4 The criticality analysis is done in a disciplined way, on the same worksheets as the FMEA. If the analysis requires updating it should be done such that any new findings are clearly stated.

4.5 FMECA should be commenced during the early stages of the design of a product/ process and the analysis should be expanded as the product or system develops. A preliminary FMECA can be performed using the limited information available during the concept stages of the design. The analysis should become more detailed as the product/ system definition improves. Eventually, the FMECA should be a comprehensive and detailed appraisal of all possible ways in which the product/process may fail and the potential consequences of these failures. The FMECA needs to be continuously updated to take account of changes to the product/system being evaluated or its intended usage.

4.6 When a criticality analysis is performed the evaluation of the criticality of each failure mode should be done in terms of worst case conditions.

5. PROCEDURE

5.1 Variations in complexity of design, and the availability of design data, will largely determine how an FMEA is performed. There are two main approaches; one based on the physical structure of the system, the other based on its functional structure.

5.2 The physical approach should be used when items within the system can be uniquely identified. The functional approach should be used if either the items do not have a unique physical identity or if the system is complex.

5.3 Each mission or mission phase and its operational modes should be identified.

5.4 The environmental profiles for each mission and mission phase should be defined. When the system is used in more than one environment, each environment should be identified together with the relevant mission phase and duration.

5.5 Functional and/or reliability block diagrams should be prepared which identify the operation, interrelation and interdependencies of the system. A number of block diagrams may be required. All inputs and outputs should be clearly shown. For clarity, a uniform identification system should be used.

5.6 The FMECA worksheets, Figure 1, should contain information on the system being analysed, the missions concerned and the date of compilation. The following should be recorded, preferably in tabular form:

a) An identifier for each item or function.

b) The function, or functions, of the item under analysis.

c) The failure modes, causes and a measure of likelihood of occurrence (see Table 1).

d) The mission phase and environment.

e) The failure effects.

f) Compensating provisions.

g) The severity rating (see Table 2).

h) Criticality (see Figure 2).

i) Detectability, e.g. Built-In Test Equipment (BITE), Automatic Test Equipment (ATE), inspection. (see Table 3).

j) A note of recommended action, e.g. design, maintenance, production, inspection etc.

Reference or Item No	Function or Process	Function	Potential Failure Mode	Potential Effect	Potential Cause	Current Control	Risk Rating				Corrective Action	Revised Risk			
							OCC	SEV	DET	RPN		OCC	SEV	DET	RPN

Figure 1 – Example FMECA Worksheet

Occurrence Rating	Description	Level*	Ranking Value	Fail Rate
Remote	Failure is unlikely. No failure associated with almost identical system.	F	1	10^{-6}
Very Low	Isolated failure associated with almost identical systems.	E	2	10^{-5}
Low	Isolated failure associated with similar systems.	D	3	10^{-4}
Moderate	Occasional failures but not in major proportions.	C	4, 5, 6	10^{-3}
High	Generally associated with systems which often fail.	B	7, 8	10^{-2}
Very High	Failure is almost inevitable.	A	9, 10	10^{-1}

* Mil Stan 1629A

Table 1 – Probability of Occurrence

5.7 All failure modes that are identified for each level of assembly or function analysed should be identified, described and analysed. Since a failure mode may have more than one cause, all probable causes at lower assembly levels or subordinate functions should be considered in the analysis, see Figure 3.

5.8 Each of the following examples of typical failure modes should be considered, this list however is not exhaustive:

a) Premature operation.

b) Failure to operate at a prescribed time.

c) Intermittent operation.

d) Failure to cease operation at a prescribed time.

e) Loss of output or failure during operation.

f) Degraded output.

5.9 The failure effects should focus on the specific assembly or function which is affected by the failure mode under consideration. But failure modes may also have effects on other levels of assemblies or functions. Therefore the effect of each failure mode should be established in terms of:

a) The local effect.

b) The effect at a next higher level of assembly or function.

c) The effect on the system and its missions.

5.10 Severity is a qualitative or quantitative measure of the consequential effects of failure modes at the total system level. The definitions of the severity categories should be agreed at the outset of the project.

Severity Rating	Severity Definition	Severity Level*	Ranking Value
Minor	It would be unreasonable to expect that the minor nature of this failure would cause any real effect on system capability. The failure might not be noticed.	Minor	1
Low	The nature of the failure causes only a slight deterioration of system capability that may require minor rework action.	Minor	2, 3
Moderate	Failure causes some deterioration in system capability which my generate the need for unscheduled rework /repairs or may cause a minor health hazard or minor injury to user.	Marginal	4, 5, 6
High	Failure causes loss of system capability or may cause a serious health hazard or serious injury to the user.	Critical	7, 8
Very High	A potential failure could cause complete system loss and/or death of user(s).	Major	9, 10

* Mil Stan 1629A

Table 2 – Example of Severity Categories

NOTE: If numerical values are assigned to severity they should follow an order of severity consistent with a measure of likelihood of occurrence.

5.11 Detection is the likelihood of controls to detect that a failure has occurred. Such detection may take many forms, i.e. BIT/BITE, lamps, alarms, visual inspection, etc. The definitions of measures of criticality should be agreed at the outset of the project.

Detection Rating	Description	Ranking
Very High	Controls will almost certainly detect the existence of a defect.	1, 2
High	Controls have good chance of detecting the existence of a defect.	3, 4
Moderate	Controls may detect the existence of a defect.	5, 6
Low	Controls have a poor chance of detecting the existence of a defect.	7, 8
Very Low	Very Low: Controls probably will not detect the existence of a defect.	9
Absolute Certainty of Non-Detection	Controls will not or cannot detect the existence of a defect.	10

Table 3 – Example of Detection Categories

5.12 Criticality is a measure of the seriousness of effect of any failure mode at the top system level and is determined from a combination of the severity and the likelihood of

occurrence of the failure mode. The definitions of measures of criticality should be agreed at the outset of the project.

6. CRITICALITY MATRIX

6.1 The criticality matrix provides a means of comparing each failure mode with all other modes for criticality. The matrix is constructed by inserting item or failure mode identification numbers in matrix locations. Conventionally, the severity category is represented on the x-axis, and probability is represented on they y-axis.

6.2 An example of a criticality matrix is shown in Figure 2.

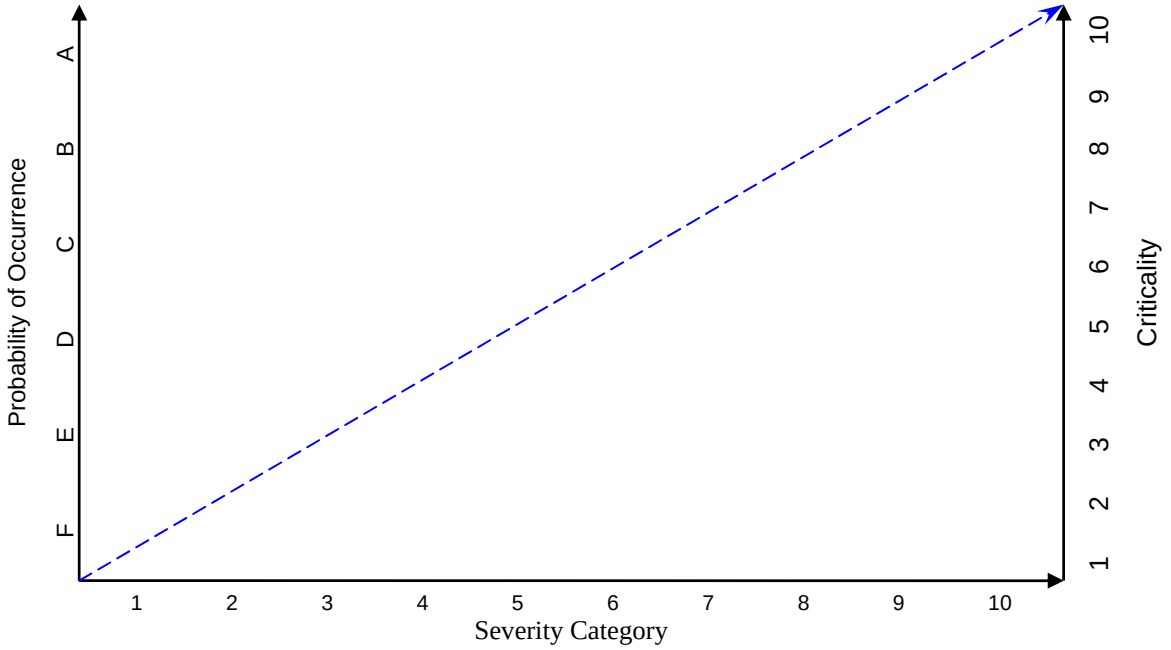

Figure 2 – Typical Criticality Matrix

7. DESIGN ACTION

7.1 A description of the way in which each failure occurs is required to ensure that the way in which the failure appears is a true indication of the failure mode. It is also important to highlight those failures which could occur but which would remain undetected.

7.2 An assessment should be made, especially for the most critical failure modes, of the action that should be taken either in terms of redesign or, where this is impossible, by means of operation action.

7.3 All failure modes which remain should be clearly stated together with the consequential effects on the system and its missions.

8. FMECA REPORT

The FMECA report should give account of or state:

a) The system description.

b) The part of the system that was analysed.

c) The assumptions made.

d) The data sources utilized.

e) The results, including work sheets.

f) Recommendations for action.

NOTE: Consideration should be given to the relative accuracy implied by any quantitative result.

9. MAINTAINABILITY ASPECTS OF FMECA

9.1 Failure Modes, Effects (and Criticality) Analyses are carried out as part of the reliability design process.

9.2 The results are used to analyse the proposed maintenance and test philosophy and to develop a reliability centred maintenance logic on which the testing, preventive Maintenance and corrective maintenance plans are based. The analysis will identify, for each failure mode, the method by which failures will be detected and located. The reiterative maintainability analysis procedure will confirm, for example, that:

a) The proposed maintenance actions conform to the maintenance requirements.

b) Each malfunction will be apparent to the operator and, if not, the analysis will indicate if a fault warning system is required.

c) The maintainer will be able to establish the location of a fault and whether it is due to a hardware, firmware or software malfunction - this in turn, will establish whether BITE or ATE is required.

d) Repair will be possible under normal maintenance conditions or whether special tools would be necessary.

9.3 These factors are fundamental to the maintainability design function and maintainability design criteria.

10. USE OF SOFTWARE

The use of either proprietary software or other tools (e.g. spreadsheets) can greatly ease the administrative and data processing tasks involved in FMECA.

11. GUIDELINES FOR REVIEWING A FMEA/FMECA STUDY

Guidelines for reviewing FMECA can be found in Part G, Leaflet 2, Attachment 1.

FAILURE MODE EFFECT AND CRITICALITY ANALYSIS

System/ Process	Hand Torch		Assessor				Date Assessed									
Subsystem /Process			Sheet				Date Reviewed									
Reference or Item No	Function or Process	Function	Potential Failure Mode	Potential Effect	Potential Cause	Risk Rating				Corrective Action	Revised Risk					
						OCC	SEV	DET	RPN		OCC	SEV	DET	RPN		
001-01		Bulb	Dim light	Dim light	Poor contacts, partially charged battery	3	5	1	15							
001-02			No light	No light	Faulty bulb, no contacts, open switch	4	7	1	28							
002-01		Switch	Stuck open	No light	Faulty switch	4	7	1	28							
002-02			Stuck Closed	Permanent light	Faulty switch	2	2	1	4							
002-03			Intermittent	Intermittent light	Faulty switch	6	4	1	24							
003-01		Contacts	No contacts	No light	Faulty contacts	4	7	1	28							
003-02			Poor contacts	Dim Light	Faulty contacts	2	5	1	10							
003-03			Intermittent	Intermittent light	Faulty contacts	6	4	1	24							
004-01		Battery	No charge	No light	Damages/Discharged battery, stuck closed switch	2	7	1	28							
004-02			Partial charge	Dim light	Correct use, Stuck closed switch	3	5	1	15							

Figure 3 – Example FMECA Worksheet for a Hand Torch

LEAFLET C33/0

REFERENCES

1 IEC 60812:2006 (BS EN 60812:2006) Analysis techniques for system reliability — Procedure for failure mode and effects analysis (FMEA), dated May 2006

2 BS 5760–5: Reliability of Systems, Equipment and Components Part 5: Guide to Failure Modes, Effects and Criticality Analysis (FMEA and FMECA). British Standards Institute. 1991..

3 Mil Stan 1629A Procedures for Performing a Failure Mode Effect and Criticality Analysis, fated 24 November 1980.

4 Mil Stan 882 Revision D, Standard Practice for System Safety, dated 10 February 2000.